DATA SECURITY: THE DISCUSSION DRAFT OF DATA PROTECTION LEGISLATION

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JULY 28, 2005

Serial No. 109–48

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE
22–989PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi, *Vice Chairman*
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *Deputy Staff Director and General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
TIM MURPHY, Pennsylvania
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas,
(Ex Officio)

JAN SCHAKOWSKY, Illinois
Ranking Member
MIKE ROSS, Arkansas
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
BOBBY L. RUSH, Illinois
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JIM DAVIS, Florida
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

	Page
Testimony of:	
Burton, Daniel, Vice President of Government Affairs, Entrust, Inc	35
Hintze, Michael, Senior Attorney, Microsoft Corporation	19
Hoofnagle, Chris, Senior Counsel and Director, Electronic Privacy Information Center, West Coast Office	27
Maier, Fran, Executive Director and President, TRUSTe	13
Additional material submitted for the record:	
Retail Industry Leaders Association, statement for the record	53

DATA SECURITY: THE DISCUSSION DRAFT OF DATA PROTECTION LEGISLATION

THURSDAY, JULY 28, 2005

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:07 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Pitts, Terry, Blackburn, Barton (ex officio), Towns, Green, Gonzalez, and Baldwin.

Staff present: David Cavicke, general counsel; Chris Leahy, policy coordinator; Shannon Jacquot, counsel; Will Carty, professional staff; Billy Harvard, clerk; Chad Grant, clerk; Kevin Schweers, communications director; Terry Lane, deputy communications director; Consuela Washington, senior minority counsel; Jessica McNiece, minority research assistant; and Edith Holleman, minority counsel.

Mr. STEARNS. Good morning. I would like to thank, first of all, the witnesses for coming before us today and to offer their comments and suggestions and helping us to craft a better bill and a workable data protection bill that will greatly improve the protection and security for all consumers and their data.

Data security breaches are an alarming trend that seems to be increasing hand in hand with the cases of identity theft and financial fraud in the United States. Identity theft and financial fraud represents the fastest growing criminal enterprise in the United States. As we learned from the Federal Trade Commission in several previous hearings, a recent survey showed that almost 10 million people in the United States discovered that they were involved in some sort of identity theft. That figure translates into almost $50 billion in losses for businesses and of course $5 billion for consumers.

Consumer data breaches and related identity theft crimes threaten not only the financial and personal security of every consumer in the United States, but also have the potential to disrupt and impede commercial activity in every sector of our economy.

Now, not surprisingly, there are now indications that consumer confidence in Internet-based and electronic transactions is starting to wane as reports mount about breaches potentially affecting millions of Americans.

Regardless of statistics and trends, I would bet that a significant percentage of us in the committee room today have been touched personally by this problem. I also believe that we can not rely solely on law enforcement and existing law for protection against breaches and related criminal activity in this area.

The Congress, and this committee in particular, is charged with the responsibility to ensure that the entities possessing and dealing in sensitive consumer data keep the doors locked and the alarm on. We intend to live up to that responsibility. The health of our modern network system of commerce demands this and all consumers deserve this.

Data, especially personal data, is the currency of the digital world. Given the sheer scope and interconnectivity of our fast-moving commercial environment, one simple mistake or oversight can leave all of us vulnerable to the lone criminal with the ability to victimize millions in an instant. Unfortunately, the crooks have discovered a lucrative new enterprise exploiting such vulnerabilities. And it is up to us to shut them down before they destroy the integrity of the data-driven commercial system that so many of us rely on.

I believe consumers, businesses, and other important stakeholders must be empowered with adequate information to assess data security risk and provide sufficient incentives to encourage the most appropriate means, technical or otherwise, to enhance data security.

My colleagues, at the most basic level, our bill would create a uniform national data breach notification regime based on risk of potential harm from identity theft. The bill also incorporates a number of provisions related to my earlier privacy bill that are intended to provide security guidelines for entities that keep personal data. I believe that once these practices are embraced, renewed consumer confidence in e-commerce and its multitude of applications will lead to even better data security in the marketplace. We need to promote the notion that security sells.

Specifically, our bill contains three major elements. The first major element of the bill directs the Federal Trade Commission to develop rules for data security, including requirements that entities in possession of personal data have a security policy, have someone designated as responsible for that policy, and have a process for taking preventive and corrective action to ensure that policy is as robust as required.

Two, the second main element of the bill relates to the special case of information brokers, which are defined in the draft as "companies whose primary business is to compile and sell consumer data to third parties". The bill requires these entities to submit their security policy to the Federal Trade Commission for audit and approval on an annual basis. In addition, any information broker is required to provide those who ask a free report of what information the entity holds on that individual.

And last, the last element establishes a national uniform standard for consumer notification when there is a security breach. A security breach is defined using a risk-based standard that relates to the probability that the security breach results in a reasonable basis to conclude that identity theft may occur. The bill requires

timely notification, both electronic and through the mail, of consumers affected.

There are also a number of provisions relating to substitute notices in cases where there is a requirement of unduly burdensome to a business given its financial conditions.

I look forward to the comments on our draft bill and would like to emphasize that the committee intends to develop this legislation through a bipartisan and open process that allows for constructive debate and discussion. We will solicit at least one or more rounds of comments and work hard to continue to refine the bill to best achieve effectiveness with this balance.

So I look forward to our testimony by our witnesses today and working together with them on this important piece of legislation.

[The prepared statement of Hon. Clifford Stearns follows;]

PREPARED STATEMENT OF HON. CLIFFORD STEARNS, CHAIRMAN, SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

Good morning. I first would like to thank the witnesses before us today as well as all who have offered comments and suggestions assisting our important work in crafting a robust and workable data protection bill that will improve greatly the protection and security of consumer data.

Data security breaches are an alarming trend that seems to be increasing hand-in-hand with the cases of identity theft and financial fraud in the United States. Identity theft and financial fraud represent the fastest growing criminal enterprise in America. As we learned from the Federal Trade Commission in several previous hearings, a recent survey showed that almost 10 million people in the United States discovered that they are involved in some sort of identity theft. That figure translates into almost $50 billion in losses for business and $5 billion for consumers. Consumer data breaches and related identity theft crimes threaten not only the financial and personal security of every consumer in America but also have the potential to disrupt and impede commercial activity in every sector of the U.S. economy. Not surprisingly, there are now indications that consumer confidence in Internet-based and other electronic transactions is starting to wane as reports mount about breaches potentially affecting millions.

Regardless of statistics and trends, I'd bet that a significant percentage of us in the committee room today have been touched personally by this menace. I also believe that we cannot rely solely on law enforcement and existing law for protection against breaches and related criminal activity in this area. The Congress and this great Committee, in particular, are charged with the responsibility to ensure that the entities possessing and dealing in sensitive consumer data keep the doors locked and the alarm on. We intend to live up to that responsibility. The health of our modern networked system of commerce demands this, and all consumers deserve this. Data, especially personal data, is the currency of the digital world. Given the sheer scope and interconnectivity of our fast-moving commercial environment, one simple mistake or oversight can leave all of us vulnerable to the lone criminal with the ability to victimize millions in an instant. Unfortunately, the crooks have discovered a lucrative new enterprise exploiting such vulnerabilities, and it's up to us to shut them down before they destroy the integrity of the data-driven commercial system that so many rely on.

I believe consumers, business, and other important stakeholders must be empowered with adequate information to assess data security risk and provided sufficient incentive to encourage the most appropriate means, technical or otherwise, to enhance data security. At the most basic level, our bill will create a uniform, national data breach notification regime based on risk of potential harm from identity theft. The bill also incorporates a number of provisions related to my earlier privacy bill that are intended to provide security guidelines for entities that keep personal data. I believe that once these practices are embraced, renewed consumer confidence in e-commerce and its multitude of applications will lead to even better data security in the marketplace. We need to promote the notion that SECURITY SELLS.

Specifically, our bill contains three major elements:

- The first major element of the draft bill directs the Federal Trade Commission to develop rules for data security, including requirements that entities in possession of personal data have a security policy, have someone designated as re-

sponsible for that policy, and have a process for taking preventive and corrective action to ensure that policy is as robust as needed.

- The second main element of the bill relates to the special case of "information brokers", which are defined in the draft as companies whose primary business is to compile and sell consumer data to third parties. The bill requires these entities to submit their security policy to the Federal Trade Commission for audit and approval on an annual basis. In addition, any information broker is required to provide those who ask a free report on what information the entity holds on that individual.
- The last element establishes a national, uniform standard for consumer notification when there is a security breach. A security breach is defined using a risk-based standard that relates to the probability that the security breach results in "a reasonable basis to conclude" that identity theft may occur. The bill requires timely notification, both electronic and through the mail, of consumers affected. There also are a number of provisions relating to substitute notice in cases where this requirement may be unduly burdensome to a business given its financial condition.

I look forward to the comments on our draft bill and would like to emphasize that the Committee intends to develop the legislation through a bipartisan and open process that allows for constructive debate and discussion. We will solicit at least one more round of comments and will work hard to continue to refine the bill to best achieve effectiveness with balance. I look forward to the testimony of our witnesses and to working together on this very important piece of legislation. Thank you.

Mr. STEARNS. And with that, the distinguished member from New York, Ranking Member Towns.

Thank you.

Mr. TOWNS. Thank you very much, Mr. Chairman.

Let me begin by first thanking you for holding this hearing. And I would like to ask to place the 43 stakeholders' comments in the record.

Mr. STEARNS. By unanimous consent, so ordered.

[The list of industry comments follow:]

DATA SECURITY DISCUSSION DRAFT—INDUSTRY COMMENTS

1. American Bankers Association; 2. Business Software Alliance; 3. Center for Democracy and Technology; 4. Consumers Union; 5. Cyber Security Industry Alliance; 6. Direct Marketing Association; 7. Dun & Bradstreet; 8. eBay Inc.; 9. Electronic Privacy Information Center; 10. Entrust Inc.; 11. Experian; 12. Federal Reserve Board; 13. Federal Trade Commission; 14. Financial Services Roundtable; 15. First Data Corporation; 16. GC Services Limited Partnership ; 17. ID Analytics; 18. IdTheftAwareness—"The Real Danny Lents"; 19. Internet Commerce Coalition; 20. Internet Security Alliance; 21. Intersections Inc.; 22. MIB Group, Inc.; 23. Microsoft Corporation; 24. National Association for Information Destruction, Inc.; 25. National Automobile Dealers Association; 26. National Business Coalition; 27. National Council of Investigation & Security Services, Inc.; 28. Peter Kiewit Institute; 29 The Progress & Freedom Foundation; 30. Reed Elsevier Inc.; 31. Retail Industry Leaders Association; 32. Software & Information Industry Association; 33. Prof. Daniel J. Solove/George Washington Univ. Law School; 34. TALX; 35. Time Warner Inc.; 36. TRUSTe; 37. US Oncology, Inc.; 38. U.S. PIRG; 39. Viacom; 40. VISA U.S.A.; 41. Vontu Inc.; 42. Wexler & Walker PPA; and 43. Yahoo! Inc.

Mr. TOWNS. Since we last met, the privacy of our constituencies have been compromised further, and their worries have increased tenfold. I was encouraged by the feedback that we received at our previous hearings. But there is much more work that needs to be done.

The discussion draft that was recently circulated includes important requirements relating to information security programs and security breach notices, but recent security breaches have revealed that consumers also care about the lack of transparency as to how

companies are using and to whom they are disclosing their personal information.

I was pleased to see that the draft includes a trigger for notification purposes. Chairman Stearns and Ranking Member Schakowsky and the rest of my colleagues would agree that this issue has haunted us for too long. It seems as though a new data security breach happens bimonthly, resulting in destroyed bank accounts and financial headaches.

As we begin to depend on technology more than ever, we must put our citizens' privacy at the top of our priority list. I hope the FTC is ready to help to stem the tide of identity theft and end the financial destruction that has plagued our constituents and web users worldwide.

I look forward, Mr. Chairman, to working with you and the members of this committee to stem this very serious problem, because the more I travel back and forth into my District on the plane and wherever, you hear these horrible stories. I think the time has come to put an end to it.

On that note, I yield back.

[The prepared statement of Hon. Edolphus Towns follows:]

PREPARED STATEMENT OF HON. ED TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Thank you Mr. Chairman for holding this important hearing. Since we last met, the privacy of our constituents have been compromised further and their worries have increased ten-fold. I was encouraged by the feedback that we received in our previous hearings, but there is much more work to be done.

The Discussion Draft that was recently circulated includes important requirements relating to information security programs and security breach notices. But recent security breaches have revealed that consumers also care about the lack of transparency as to how companies are using and to whom they are disclosing their personal information in the first place. I was pleased to see that the draft includes a "trigger" for notification purposes. No one likes to be inundated with dozens and dozens of risk-related notices, and I agree that warnings should only be sent when there are severe breaches capable of significant consumer burden.

I think that Chairman Stearns, Ranking Member Schakowsky and the rest of my colleagues would agree that this issue has haunted us for too long. It seems as though a new data security breach happens bi-monthly, resulting in destroyed bank accounts and financial headaches.

As we begin to depend on technology more than ever before, we must put our citizens' privacy at the top of the priority list. In July 18th's Wall Street Journal, Bill Hancock, Chief Security Officer of Savis, Inc., a major internet service provider, is quoted as saying, "What people can do on computer networks and what they can find has increased ten-fold from a few years ago." He went on to state that "Evil intent is easier than ever."

I hope the FTC is ready to help to stem the tide of identity theft and end the financial destruction that has plagued our constituents and web users worldwide. I look forward to monitoring the positive developments that are sure to stem from our committee draft.

Thank you.

Mr. STEARNS. I thank my colleague.

The gentleman, Mr. Pitts, is recognized.

[No response.]

Mr. STEARNS. The gentleman waives.

Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much, Mr. Chairman.

Again, I commend your continuous efforts. You have been on this issue for some time, and I appreciate you calling this particular

hearing. I will be brief, but I will also request that my written statement be submitted in its entirety by unanimous consent.

Mr. STEARNS. With the record's consent, so ordered.

Mr. GONZALEZ. I guess what we are trying to find out today, and I appreciate the presence of the witnesses. Many times I feel that you all come here and give us the benefit of your knowledge and experience, and then you feel that maybe we are not listening, but the truth is, we have a record, we have your statements, and we do make reference to them as we proceed with this piece of legislation.

My only observation is that we deal with this in a realistic framework and that is what is happening out there, what is it possible that you bring to this. We need your suggestions and recommendations. And that our policies will affect the abilities that technology give us today, we can't go out there and impose on what is going on out there in commerce and such, conditions that could never be met, technologically or otherwise. But I think that there can be certain compromises that still address the chief concerns as expressed by my constituents when we have town hall meetings.

The greatest attendance that I have had in any town hall meeting, I guess second to Social Security, has been ID theft. It is out there. It is tremendous. And working together, hopefully we will come up again with a feasible, viable answer. The problem with technology, and I have said this before about technology, I guess it is the old proverbial key that opens the gates to paradise, but it is the same key that can open the gates to hell. And so somehow, we avoid that and do the best that we can.

And again, thank you very much for your participation, and I yield back.

[The prepared statement of Hon. Charles A. Gonzalez follows:]

PREPARED STATEMENT OF HON. CHARLES A. GONZALEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, thank you for holding today's hearing on the discussion draft data protection bill that this subcommittee is developing. I would particularly like to thank both the majority and minority staff for their work on this. I know that they have been called upon in recent days and weeks to put many hours into other legislative items related to the Energy and Commerce Committee, so I especially appreciate their attention to this legislation. This discussion draft provides us with an excellent starting point for addressing the rash of data breaches that have been threatening the privacy and financial standing of consumers across America. I look forward to working with you, Mr. Chairman, the Ranking Member, and other members of this subcommittee to further build on the draft before us today.

The problem of data security, and the risk of identity theft that it carries, is a serious concern to people. I know that in my own district in San Antonio, public attention is strong. I held a town hall meeting in my district in May, which brought together the Federal Trade Commission and federal and local law enforcement. The turnout from the public was impressive. And despite being in an auditorium without air-conditioning for over two hours, almost the entire audience stayed to the very end and asked many questions. The bottom line is that people want assurances that their private information is handled securely and that breaches in data security are handled swiftly and effectively.

As we move forward with this legislation, I hope that we can have an end-product that adheres, as much as realistically possible, to the principle of "don't collect it if you can't protect it." In other words, companies and organizations should not be collecting personal information from individuals if they are not going to be able to reasonably ensure the security of that information.

In addition to the provisions already in the discussion draft, I would like to also consider several related issues. First: how we deal with paper records. "Dumpster diving" is a prevalent practice in which identity thieves go through dumpsters to

find documents with individuals' personal information. San Antonio local law enforcement has cited this practice as one of the most prevalent forms of identity theft. We should explore the feasibility of including provisions in this bill to require companies to shred or otherwise destroy documents with individuals' personal information before throwing them away.

Second, the draft bill gives the individual the right to get a free report on what data the information broker companies hold on that individual. If individuals feel the information in the broker's database is inaccurate, they should be able to add supplementary information to their file to clarify the existing information.

Third. Under the draft bill's data breach notification requirements, a "substitute notice" system is established for companies that cannot afford to send a letter to every individual affected by a breach, or if they do not have complete addresses for those individuals. Substitute notification consists of the company alerting the media and posting a message on their website. We may want to consider whether the bill should also require that these companies notify the FTC and that the FTC maintain a central public website listing all data breaches, along with information for consumers on how to contact those companies and determine if their own personal data was compromised. I know that private websites with a similar intent have been established, but it may strengthen consumers' confidence to have such a function permanently and reliably carried out by the FTC.

Finally, as I represent a district with a sizable population of Spanish-speakers, I would like to explore how we can ensure that these consumers and other language minorities, who are heavily targeted by companies for their business, are able to access notices sent to consumers about data breaches. We need to ensure that these notices are available in a language that these consumers can understand.

Thank you Mr. Chairman. I look forward to hearing from our witnesses today, and to working with you on this subject.

Mr. STEARNS. The gentleman yields back.

The gentlelady from Tennessee is recognized.

Ms. BLACKBURN. Thank you, Mr. Chairman.

I want to thank the chairman for holding this hearing and for the witnesses for taking your time and being here with us today.

Many constituents in my District have expressed to me their concerns about identity theft, and we recently held a workshop, an identity theft workshop, in our District. It was enlightening. It was well attended. And it was something that we gained some information from, so we are looking forward to hearing what you have to say. And as this committee examines steps to prevent identity theft, we must ensure that companies and individuals are not burdened with unnecessary regulations, but that they have opportunities for privacy protection.

Congress should focus on reasonable security measures that will protect personal information and provide enforcement mechanisms to penalize companies that readily buy and sell information on us to unscrupulous entities who will exploit our identities for their personal gain.

Today, this committee looks at draft legislation on data security, which I believe is a good step, a good first step, in addressing the problem. I commend Chairman Barton and our subcommittee chairman for their efforts on this issue.

And again, I thank you. We look forward to hearing your input. Thank you.

Mr. STEARNS. Thank you.

The gentlelady from Wisconsin.

Ms. BALDWIN. Thank you, Mr. Chairman.

I am also pleased that we are having this hearing today, Mr. Chairman, and our witnesses.

This is an increasingly important question how we protect our sensitive personal information from theft and abuse. And the sta-

tistics are staggering. The 10 million Americans who were affected by identity theft in the year 2004, it is pretty staggering. Access to the right data bases and the touch of a button or two allows access to vast amounts of information about a person, things like date of birth, Social Security number, credit rating, debts, loans, insurance claims, magazine subscriptions, even DNA.

American consumers deserve to have their personal information protected. And I am pleased that our subcommittee will act soon to address this. And I also agree that the discussion draft before us is a good first step.

But as we consider next steps, changes, modifications, there are a number of issues that we need to address and questions we will need to answer, questions such as should we preempt State laws, and if so, how broad a preemption is appropriate. When should consumers be notified of data breaches and who decides? Should the FTC maintain public notices, public information about data breaches? Do we need to reach beyond our committee's jurisdiction to adequately address this problem? Should we exempt encrypted data? What role should States have in prevention and enforcement?

So today, I hope our witnesses will articulate ways in which we can protect consumers from identity theft and misuse of their personal data and hopefully help us explore the answers to those questions.

Thank you, Mr. Chairman, I yield back.

Mr. STEARNS. I thank the gentlelady.

Mr. Green, the gentleman from Texas.

Mr. GREEN. Thank you, Mr. Chairman. I would like to thank both you and our ranking member for taking lead on this issue and holding this important hearing.

I would like to welcome our witnesses and thank you for your cooperation and being here and sharing your knowledge and experience. It is imperative for us when we begin drafting legislation to combat identity theft and data theft that we have the experience from the business community, so we make sure we pass legislation that really will do the job and again still allow us to enjoy the benefits of what we do.

The committee has held four hearings since the fall of 2004, and we have had a lot of discussions on passing a bill on data security, and I believe the bill, as drafted, is a good start.

I want to bring up a couple of issues, though, I have some concern on. The preemption issue, special attention to that provision. Currently, several States have stronger policies when it comes to data security that we are proposing, and we are proposing, furthermore, 18 States that have passed breach notification laws, all of them, including my home State of Texas, offer an encryption safe harbor.

And I believe you should look at issues such as encryption and mask data to serve as a second form of defense. It is frustrating, because in March we heard testimony from Choice Point and Lexus Nexus, because both of these companies had a recent experience of breach in their security, and at that time, Lexus Nexus had almost 32,000 people affected. Well, then a few weeks later, we really found out it was 300,000 that may have been affected by the

breach in security. And identity theft is the No. 1 crime in our country. In fact, it is getting worse all of the time.

In our District, we have done identity theft workshops for our constituents, but you know, it is a very small group. We have to do something more for the mass of people who have that fear. And these workshops, even those only work when credit-reporting agencies and financial institutions and data brokers do their job to make sure information doesn't fall into the wrong hands. We are all a number now, and most often, it is our Social Security number, and every financial institution uses that number, including when I had to rent a U-Haul truck, Mr. Chairman, they wanted my Social Security number. And I said, "Why?" And they said, "Well, we just require it." And I said, "Well, I don't want to rent the truck." And they said I didn't have to. And that is what I suggest to my constituents. If it doesn't have anything to do with taxes or payroll, then just say no, or credit. And you can do that. But I still like to get the credit to use some other identifying number. And I know a lot of States are working on that.

Our current systems of laws addressing the problem are piece meal. We have the Fair Credit Reporting Act. We have the Federal Trade Commission that addresses unfair and deceptive practices. We have separate laws and driver's license data. So what we need to do, Mr. Chairman, I am glad you are taking the lead in putting this together. And I would hope we would still look at empowering the States and just an example, when Congresswoman Heather Wilson and I worked on the stand for so many years, we ended up the compromises that we wanted uniform standards around the country, but we also still empowered the State Attorney Generals to be able to do their job as consumer representatives, but they had to use Federal law to do it. And as long as we pass a strong law and still empower the States in addition to whatever the FTC or whatever agency we give this authority to.

But I look forward to participating and working on not only the hearing today but also in the drafting of legislation.

Thank you.

Mr. STEARNS. I thank the gentleman. And I thank him for considering ways to do this in a bipartisan fashion.

I don't think there are any more members, so let me welcome——

Mr. TOWNS. Mr. Chairman, will you yield for one moment?

Mr. STEARNS. Yes. Yes.

Mr. TOWNS. I ask unanimous consent that we place the statement of Ranking Member Jan Schakowsky in the record. She has a family emergency.

Mr. STEARNS. I heard that, and I am sorry to hear that. So with unanimous consent, so ordered. I appreciate you doing that.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Chairman Stearns, for holding this hearing today and for your good leadership on data security issues. Millions of records in other people's computers define and describe our lives. The recent rash of security breaches has made us keenly aware of just how vulnerable our records are to release through inept data security practices or, worse, intentional theft. Past hearings at this Subcommittee

have explored those breaches and exposed the gaps in protection. Today, the Committee puts forth a bipartisan draft that aims to fill the gaps in protection. I want to thank Chairman Stearns, Ranking Member Schakowsky of the subcommittee, Ranking Member Dingell of the full committee, and all of the staffs for their work on this bipartisan discussion draft.

I am pleased with the careful consideration this Committee is giving to this important issue. Our goal is to work with industry and consumer groups in developing this legislation to encourage a culture of strong data security. Data security has not been the priority it ought to be and must become. I hope that the testimony we receive here today will help us to perfect the draft bill.

There are two critical components to the draft bill:

- One, a legal requirement for establishing and implementing information security practices; and
- Two, notification requirements in the event of a security breach.

In mandating information security policies, we hope to strike the right balance between ensuring real protection for consumers without halting the evolution of technology and best practices. We would be remiss not to mandate robust security for personal information, but we'll do it in a way that allows companies to implement the security measures most effective for the types of information they maintain.

I would like to point out that the draft bill does not yet include guidelines for what companies must include in their information security policies. I believe guidelines similar to those of the FTC's Gramm-Leach-Bliley Safeguards Rule are a good place to start. I request that our panel of experts provide the Committee with some guidance on this issue. Over the August recess, we will be perfecting the draft and readying it for introduction, and your guidance will be an important part of that preparation.

We have also been careful in crafting the notification requirements of the bill. While consumers ought to be notified when a breach of their information puts them at risk for identity theft, they should not be showered with warnings when there is no risk. The notification requirement of the bill has a trigger to avoid both "over-notification" and "under-notification". The bill provides that notice should be prompt and meaningful so that consumers can best shield themselves from identity theft.

The draft bill also places additional requirements on information brokers, those who trade in non-customer data. Because the normal market incentives for protecting customer information are absent or diminished with this business model, the draft imposes federally supervised security audit requirements for these entities.

I plan to move data security legislation though this Committee in September, and I hope that we can get a bill signed into law this Congress. I would also like to mention that I support Congressman Clay Shaw's bill protecting individual Social Security numbers. I will do my part to quickly move the portions of the bill that are within our Committee's jurisdiction, once we get a referral of the bill.

I thank the witnesses for participating in the hearing today and look forward to your testimony on the draft legislation. Thank you Mr. Chairman, I yield back the balance of my time.

PREPARED STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Thank you, Chairman Stearns, for holding today's hearing on our draft legislation to address the recent spate of security breaches of personal information. I would also like to thank Chairman Barton and Ranking Member Dingell for working with us to protect consumers' personal information where current business practices and data security laws have failed to do so. The time has come for us to ensure that personally-identifiable information is protected and that consumers are notified when their information has been compromised.

In the last five months alone, over 50 million consumers have had their personal information lost, stolen, hacked into, exposed online, or sold by corrupt insiders—and through no fault of their own. Personal information is being collected, transferred, and sold everyday. Consumers are told that if they want to rent an apartment, buy a pair of shoes, or contribute to a university, they have to divulge their name, address, Social Security number, credit card number, mother's maiden name—and more—just to do so.

So many consumers are willing to provide the key facts of their lives because they believe that since they are dealing with a well-known retailer, their alma mater, or an established bank, their personal information will be treated as just that—personal—and that it will be secure. Until recently, most people had no idea that the

teenage hacker looking for some kicks and the most sophisticated crime rings alike were raiding the virtual treasure troves of personal information at businesses, universities, and information brokers. But, news of the breaches at DSW, Bank of America, and Boston College, to name a few, has made consumers and Congress alike realize that more needs to be done to protect consumers' personal information.

The bill we have been working on seeks to stop the pillaging of personal information by raising the bar for the handling and security of consumers' data. It seeks to make information brokers—those whose business is to turn your name into a commodity—more accountable to consumers. The bill would also take California's groundbreaking idea—that consumers have a right to know when their information has been compromised—and turn it into the standard for our country.

The draft at hand is a good start, but we have to do more to make sure that we provide the best protection for consumers that we can. When we consider the scope of the information our bill covers, we need to remember that it does not matter to the victim of identity theft where their information was stolen from -a small business or a massive data broker, and it does not matter what form it was in—paper or electronic. It does not matter if access was gained by an outsider who was not authorized to do so or an insider who had the key to the encryption code. It does not matter if their file was the only one compromised or if it was one of thousands. We also must keep in mind that identity theft is not the only threat with which we should be concerned. Information in the wrong hands could put domestic violence and stalkers' victims' lives at risk.

Additionally, consumers need to know more than that their information is secure. Since data brokers sell personal information to those who will decide whether consumers will get jobs, roofs over their heads, and even whether they have the legal right to vote, consumers must have the right to make sure that the information that is meant to represent what kind of risk they are to employers, landlords, and the local government is correct.

We have heard claims from information brokers that allowing consumers to correct their files would be difficult to do because much of the data they have is from public records and the brokers do not have the legal authority to correct them. However, I believe we should not throw up our hands and say that nothing can be done. I believe that if consumers question the accuracy of their files, data brokers could—at a minimum—"flag" that information to let those using the files know that there is a question of the accuracy of the file. And, a common problem with inaccurate reports is not that the original record is incorrect, but that one person's file has been mixed with another's. For instance, my file may be mixed with a Jean Schakowsky's or Jan Stockowski—or both. I believe that data brokers should be compelled to fix those "mixed files." Consumers must have every opportunity possible to set the record straight because of the impact incorrect information can have on their lives.

Finally, I believe it is important that we establish a strong federal standard so that we do not have to worry about preempting 50 state laws. While I can understand the desire to see one federal standard, I believe that if we set the floor high enough, states will not have to go beyond our requirements. Because so many states have beat us to protecting consumers—including Illinois, Florida, and Texas— I believe we must exercise great caution when we consider how we will contend with state laws on data security and breach notification.

Once again, Mr. Chairman, I look forward to working with you on our common goal of protecting consumers. Although there are many issues that are still on the table, I think that using consumers' rights and safety as our guiding principles, we will be in good shape. Thank you.

PREPARED STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MASSACHUSETTS

Mr. Chairman, thank you for holding this important hearing today.

Mr. Chairman, on March 15th, following massive breaches of personal information at ChoicePoint, Bank of America and LexisNexis, you wisely convened a hearing in this Subcommittee to question executives from major data profiling firms. This hearing provided important momentum for ongoing efforts to strengthen privacy protections for the millions of Americans whose private information is gathered by data merchants who view our Social Security numbers, credit records and other sensitive personal information as commodities to be bought and sold for a profit.

Since the Subcommittee hearing, a tidal wave of personal data has gushed from a long list of data brokers, public companies, universities, financial institutions, high schools, hospitals and other organizations. The Privacy Rights Clearinghouse

has reported that *more than 48 million personal records* have been lost or stolen *over the past four months alone.*

Mr. Chairman, today's hearing on draft legislation you are preparing in collaboration with the Democrats on the Committee is another step towards providing Americans with increased control over their most precious and private personal information. I commend you for your efforts to date.As you know, Mr. Chairman, the draft bill defines personal information as "an individual's first and last name in combination with any 1 or more of the following data elements for that individual: Social Security account number, driver's license number or other State identification number, financial account number, or credit or debit card number' that would enable access to an individual's financial account. [Sec. 5. Definitions, Page 9]. The bill also permits the Federal Trade Commission to modify this definition. [Sec.5. Definitions, Page 11].

Last week, the full Energy and Commerce Committee marked up H.R. 1132, legislation to provide grants to states for building or enhancing state-run prescription drug databases. These databases will contain personal information about patients—their name, address and phone number—along with the type of prescription, quantity dispensed, the number of refills and related data about the drugs they are prescribed that are subject to the bill's reporting requirement.

I appreciate the Chairman's comments during last week's mark-up about the importance of securing this health information and notifying patients in the event that their electronic medical records are lost, stolen or used for an unauthorized purpose. As the data security bill before this Subcommittee evolves, I look forward to working with the Chairman to ensure that consumers' medical information is covered by the protections contained in this bill.

I would also like to point out a few other areas of this draft legislation that deserve further review and adjustment.

1. *The scope of the bill:* As noted in the testimony provided by Fran Maier of Trust-e (TRUST-E), it appears that the bill, in its current form, does not cover personal information held by banks, unions, thrifts and government entities like the state-run databases that maintain records on patients and the prescription drugs they take. I agree with the Mr./Ms. Maier that when a consumer's personal information is leaked from a database, it matters not whether the information was leaked from a bank or a university or a state's department of health. This bill's privacy protections should be brought to bear whenever a consumer's personally-identifiable information is lost, stolen or divulged for an unauthorized purpose.

2. *Pre-emption of state law:* I am concerned that this bill would pre-empt stronger state laws. For example, because California has a law that requires consumer notification in the event of data breaches at financial firms and government institutions, consumers in California would be denied this protection if this bill were to become law, since it contains no such coverage and would pre-empt the California statute.

3. *The trigger for notification:* While the method and content of the consumer notification requirement in the bill is specific and detailed [Page 5], the conditions that trigger this notification are murky. For consumers to be notified of a breach that affects their personal information there must be a compromise of security that results in "the acquisition of personal information by an unauthorized person that may result in identity theft." [Page 5] I would suggest that this trigger be expanded so that notification would occur if the information were lost, stolen or used for an unauthorized purpose. The "identity theft test" is too difficult to determine, particularly in the immediate aftermath of a breach, and there is other damage—beyond identity theft—that can be inflicted upon consumers by the misuse of their personal information. Consumers should be notified in these instances too, even if the breach may not result in someone stealing their entire identity.

I commend the gentleman from Florida, Chairman Stearns, for holding today's hearing, and I look forward to working with you to refine this bill. I appreciate the witnesses appearing before us this morning and look forward to their testimony.

Thank you.

Mr. STEARNS. We will ask the witnesses to come forward. We have Ms. Fran Maier, Executive Director and President of TRUSTe, San Francisco, California; Mr. Michael Hintze, Senior Attorney, Microsoft Corporation, Redmond, Washington; Mr. Chris Hoofnagle, Electronic Privacy Information Center, Senior Counsel and Director, West Coast office in San Francisco; and Mr. Daniel Burton, Vice President of Government Affairs, Entrust, Inc., McLean, Virginia.

Ms. Maier, we welcome your opening statement.

STATEMENTS OF FRAN MAIER, EXECUTIVE DIRECTOR AND PRESIDENT, TRUSTe; MICHAEL HINTZE, SENIOR ATTORNEY, MICROSOFT CORPORATION; CHRIS HOOFNAGLE, SENIOR COUNSEL AND DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER, WEST COAST OFFICE; AND DANIEL BURTON, VICE PRESIDENT OF GOVERNMENT AFFAIRS, ENTRUST, INC.

Ms. MAIER. Mr. Chairman——
Mr. STEARNS. Yes, there is a little switch there.
Ms. MAIER. Hello.
Mr. STEARNS. Yes.
Ms. MAIER. Thank you.
Mr. STEARNS. Yes, that is good.

Ms. MAIER. Mr. Chairman, and members of the subcommittee, Ranking Member Towns, I want to thank you for the opportunity to address you today on this important proposed legislation and to tell you about TRUSTe's security guidelines, which we released earlier this year.

TRUSTe is an online privacy leader. We have been around since 1997 as an independent, non-profit organization. As you mentioned, we come from San Francisco, adjacent to Silicon Valley, and we have been very close to the issues related to California's State Bill 1386.

Our mission is to enable individuals and organizations to establish trusting relationships based on respect for their personal identity and information in the ever-evolving networked world. We are very concerned about Internet, and we are very concerned about trust and e-commerce.

We have over 1,500 companies, their websites, who have been certified by TRUSTe's process and carry the TRUSTe trustmark, the green and black symbol you have seen. We are also approved as a safe harbor for Children's Online Privacy Protection Act with the FTC and by the U.S. Department of Commerce for the EU Safe Harbor.

We are also deeply involved in e-mail practices. For example, we just launched a new e-mail privacy seal for websites, which is based on permission from consumers and allows a company to post a seal that says, "We don't spam," if they meet the strict standards that we require. We also serve as an e-mail accreditation authority for Bonded Sender, one of the leading legitimate e-mail sender programs. Again, this is to address another issue that faces consumers in terms of spam.

My remarks today will be brief and will focus first on TRUSTe's security guidelines and then specific thoughts on the proposed legislation.

Our security guidelines were released in March of this year in consultation with many of our shareholders and others in industry. As you well know, privacy is closely intertwined with security. You can't really deliver privacy unless you have security. Security is necessary but not sufficient to deliver acceptable privacy to consumers. So we felt that it was very important for us to address security and to provide some guidelines for our members who are obviously engaged in and value privacy.

The guidelines, of course, are expected to evolve, much as we expect this legislation to evolve, to address new technologies, new threats, and new consumer concerns. The guidelines are drafted in checklist form, and the reason why that is important is because small companies and large companies, depending on the size, depending on the kind of information they collect, might have different reasons or different expectations for the kind of security that they should abide by. Larger, more complex companies which handle data with the highest level of sensitivity will likely find it appropriate to adopt all of the recommended practices. However, smaller companies collecting less sensitive information may conclude that adopting only some set of these controls will still enable it to have a security program appropriate to the nature of data it collects and its consumers.

The guidelines like the FTC's guidelines and others echo the structure that you could find at those other pieces of rules. For example, we have administrative rules. This includes drafting an internal security policy and appointing someone to be the executive in charge of security, which is similar to what you have proposed in the legislation before us. Administrative controls also include training of employees and other items such as procedures internally. Of course, a big part of security guidelines includes tentacle measures. This includes password practices, controlling employee access to sensitive information, ongoing monitoring, firewalls, vulnerability testing, and the like, and then finally physical controls which include monitoring access to data, securing one's data facilities, and those kinds of physical things, covering not only electronic data but also paper-based data.

All of these guidelines can be found within TRUSTe's testimony that we submitted, and of course, on our website.

Now let us turn to the proposed data protection breach notification legislation. We, of course, would like to applaud the committee on its hard work on the draft legislation. We believe that this is the right balance and mandates high standards and allows for flexibility in their implementation. And we think it also provides the right incentives for companies to put meaningful security safeguards into place in their own and consumers' best interests. We believe that the desire to minimize a potential negative publicity, brand damage, and embarrassment often resulting from the disclosure of a data breach has been proven to motivate companies to prioritize security much more highly than they otherwise would.

We wish to focus on a couple provisions of the bill today.

First of all, in terms of the scope of the legislation and the trigger for security breach. We appreciate, first, that the committee has put focus on the jurisdiction for the industry under which it has jurisdiction. However, from a consumer's perspective, when their information is breached, the particular industry or organization involved is irrelevant to them. We believe that consumers should enjoy the same level of protection regardless of the industry involved. So we would recommend that the jurisdiction extends to the financial services especially.

In a related way, we would like to express concern about the scope and the definition of person under Section 5 Subsection 6 of the bill. We would urge the committee to expand the definition so

that the scope of the legislation covers local, State, and Federal law. As you know, in California, it does cover the State government, which is really where the legislation in California came from.

The second point that we would like to talk about is the definition and notice of breach of security. The current draft includes a trigger requirement for notice as a result in or there is a reasonable basis to conclude has resulted in the acquisition of personal information by an unauthorized person that may result in identity theft. The qualifier language "that may result in identity theft" we believe is subjective. Whether something may result in ID theft depends, in a large part, on the sophistication of the wrongful acquirer of the data. It is not feasible for the potential provider of the breach notice to definitively assess the skill level and sophistication of the wrongdoer and certainly not an intermediate aftermath of a breach, which is when such an assessment would have to be made.

We would recommend the committee to consider altering this definition with a qualifier that is a bit more broad, one that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such personal information.

There has been a question of whether or not a broader definition or a broader trigger may result in too many notices to consumers. We believe that the experience in the State of California, which the law has been in effect for over 2 years, seems to have struck the right balance. Consumers are receiving appropriately useful notices, and based on our own observations as well as our consultations with the staff of the California Office of Privacy Protection, that the law has not resulted in a——

Mr. STEARNS. Ms. Maier, if you could, just sum up.

Ms. MAIER. That is great, sir. Thank you.

Again, I very much appreciate being here. We look forward to working with you and hopefully discussing the creation of a safe harbor. And we thank you.

[The prepared statement of Fran Maier follows:]

PREPARED STATEMENT OF FRAN MAIER, EXECUTIVE DIRECTOR AND PRESIDENT OF TRUSTE

Chairman Stearns, Chairman Barton, Ranking Member Schakowsky, and members of the Subcommittee, I am Fran Maier, Executive Director and President of TRUSTe. I thank you for the opportunity to address the Subcommittee on this important proposed legislation and to tell you about TRUSTe's Security Guidelines, which we released earlier this year. TRUSTe is an independent, nonprofit organization with the mission to enable individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. Through long-term supportive relationships with our licensees, extensive interactions with consumers in our Watchdog Dispute Resolution program, and with the support and guidance of many established companies and industry experts, TRUSTe has earned a reputation as the leader in promoting privacy policy disclosure, informed user consent, and consumer education.

TRUSTe was founded in 1997 to act as an independent, unbiased trust entity, and we have earned our reputation as the leading builder of trusting relationships between companies and consumers. The TRUSTe privacy program—based on a branded online seal, the TRUSTe "trustmark"ridges the gap between users' concerns over privacy and Web sites' needs for self-regulated information disclosure standards. In May 2001, the Federal Trade Commission approved TRUSTe's Children's Privacy Seal Program as a safe harbor under the Children's Online Privacy Protection Act. We are proud to have received that designation. Hundreds of thousands of young children who are active online are protected by our program, which currently includes some of the most popular Web sites, including www.disney.go.com,

www.kids.msn.com, and www.epals.com. TRUSTe is also certified as a safe harbor program under the Safe Harbor Framework administered by the U.S. Department of Commerce for U.S. companies wishing to receive personal data from countries in the European Union ("EU"). Our EU Safe Harbor Seal Program gives companies assurance that they are in compliance with the Framework and, therefore, with national data protection laws in all EU member states.

In addition to these efforts, TRUSTe is deeply involved in fostering best practices for email. We have just launched our permission-based Email Privacy Seal Program, which allows companies who agree to our strict standards to post a TRUSTe "We Don't Spam" seal on online and offline forms where they collect email addresses. We also serve as the email certification authority for senders of legitimate email who are members of the Bonded Sender Program.

Finally, we are a California company, and we closely follow developments in California law, including the data breach notification law, to keep our licensees informed about compliance issues. We also work closely with the California Office of Privacy Protection in its ongoing efforts to provide guidance to businesses and consumers on privacy and security issues.

TRUSTE'S SECURITY GUIDELINES

In March of this year, TRUSTe issued our first version of Data Security Guidelines. As the Committee recognizes, privacy is very closely intertwined with security. We believe that security is necessary but not sufficient to giving consumers the privacy assurances they expect. In developing the Guidelines, we aimed to expand the reach of our expertise in privacy by providing our licensees and other members of the public a resource they can use as a foundation of responsible data security practices.

The Guidelines are divided into three categories of safeguards: administrative, technical, and physical controls. This structure echoes that of the Federal Trade Commission (FTC's) Gramm Leach Bliley Safeguards Rule, which we discuss in further detail below. Administrative controls include, for example, drafting a written internal security policy, training employees, conducting ongoing security risk assessments, and establishing procedures in connection with external third parties (including vendors) with whom data is shared. Technical measures include controlling employee access to sensitive information on a need-to-know basis, establishing good password practices, ongoing monitoring to assess threats and vulnerabilities, and establishing incident response procedures. Finally, physical controls include practices such as monitoring legitimate access to data, establishing physical access controls, and securing one's data facilities.

The Guidelines are drafted in checklist form so that companies can assess their own risk levels and adopt the corresponding appropriate level of recommended safeguard practices. Larger, more complex companies which handle data with the highest level of sensitivity will likely find it appropriate to adopt all the recommended practices, while a smaller company, collecting less sensitive information, may conclude that adopting only a subset of these controls will still enable it to have a security program appropriate to the nature of the data it collects and handles.

We anticipate that our Guidelines will evolve over time to reflect emerging technologies and business issues that may impact the safety, security and quality of sensitive or confidential information used by TRUSTe's licensees. We have attached the Guidelines as an appendix to our testimony, for the Committee's review. The Guidelines are also posted on our Web site at http://www.truste.org/pdf/SecurityGuidelines.pdf.

THE PROPOSED DATA PROTECTION AND BREACH NOTIFICATION LEGISLATION

TRUSTe applauds the Committee on its work on the draft legislation to date. We believe the bill strikes the right balance by both mandating high standards and allowing for flexibility in their implementation. As a result, the bill provides the right incentives for companies to put meaningful security safeguards into place in their own, and consumers', best interests. In addition to imposing security standards directly, we believe the draft legislation will fundamentally empower consumers to take action to minimize the potential impact of ID theft. The desire to minimize the potential negative publicity, brand damage, and embarrassment often resulting from the disclosure of a data breach has been proven to motivate companies to prioritize security. The market-driven, non-prescriptive approach you have chosen will encourage companies to protect personal information.

We wish to highlight a few specific provisions in the bill.

SCOPE OF THE LEGISLATION

As the bill's jurisdictional limits are those of the Federal Trade Commission Act, it does not cover banks, unions, thrifts, and common carriers. We appreciate that the Committee has crafted a bill that applies to industries under its jurisdiction, and we understand that the House Financial Services Committee, and the Senate Banking Committee, are working on parallel legislation governing entities within their jurisdiction. We support these efforts. From a consumer's perspective, when a database is breached, the particular industry involved is irrelevant. We believe that consumers should enjoy the same level of protection, regardless of the industry involved.

Thus, we believe that the legislation's requirements should extend across all industries. For instance, insurance institutions would not be reached by the scope of this bill. Those financial institutions that are regulated under the Gramm Leach Bliley Act have no requirement to provide breach notices; therefore it would be appropriate to exempt financial institutions from the requirements of section 2, but not from section 3. In fact, were this legislation to become law with the current preemption language, California residents would have less protection than they do now under the California data breach notification statute since it applies to financial institutions. In the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501-6505, Congress gave enforcement authority to the appropriate regulatory agencies over industries not regulated under the FTC Act. Perhaps the COPPA model could be followed here.

The Committee has doubtless considered the role of vendors or service providers in the context of breach notices. The Federal Trade Commission (FTC's) GLB Safeguards Rule expressly recognizes the responsibility which principals must take for the security practices of their service providers (section 314.4(d)), and we recommend that the Committee consider adhering to this philosophy in the context of this legislation, also.

The California data breach notification statute imposes specific responsibilities on service providers (i.e., those not having a direct relationship with the consumer, and acting on someone else's behalf) to notify the party who *does* have the direct relationship. This allows the principal to maintain control of the notification process, and ensures that it has the right to be notified itself in case of a breach by a service provider. The California law defines service providers as those who do not "own" the data in question. Since in the customer's eyes their relationship is with the principal, from the customer's perspective, the principal is *responsible* for the service provider's breach. If the consumer has a relationship with the company (i.e., it's not a data broker situation), then it is proper for the consumer to hear about the breach from the principal, and not from an unknown third party service provider.

Finally, we would like to express concern about the scope of the definition of "Person" under Section 5(6) of the bill. This definition as defined in 551(2) of title 5, United States Code, does not include any governmental agency. We would urge the Committee to expand that definition so that the scope of the legislation covers local, state and the Federal government. Again, enactment of the legislation as drafted with the current preemption provision would weaken consumer protections currently provided by the California breach notification statute, which extends to governmental agencies.

DEFINITION OF "BREACH OF SECURITY"

Section 3 of the bill would impose certain notice requirements upon companies that discover there has been a "breach of security" affecting their databases. Although the specific facts and circumstances that constitute a "breach of security" are left to rulemaking by the Federal Trade Commission, the legislation requires, at a minimum, that a breach triggering the notice requirement "result . . . in, or there is a reasonable basis to conclude has resulted in, the acquisition of personal information by an unauthorized person that may result in identity theft." Section 3(b) (emphasis added). The qualifier language "that may result in identity theft" in the proposed legislation is subjective in nature. Whether something may result in ID theft depends in large part on the sophistication of the wrongful acquirer of the data. It is not feasible for the potential provider of the breach notice to definitively assess the skill level and sophistication of a wrongdoer, and certainly not in the immediate aftermath of a breach—which is when such an assessment would have to be made.

We think the Committee should consider altering this definition with the qualifier "that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such [personal] information." This would mirror the approach taken in the FTC's *Guidelines.* If this approach is taken, the standard could become a ceiling for the level of protection granted, eliminating the need for the FTC to re-

vise the standard through future rulemaking. Rather the FTC could develop guidelines that would be instructive in their nature and perhaps fit into a safe harbor program which we address later in our testimony. TRUSTe believes that this approach provides strong protection for consumers and would not likely lead to an overload of notifications. It also provides certainty for businesses who may be concerned about the standard changing in the future.

The parameters of the California security breach notification law are instructive in this regard. California Civil Code Sections 1798.29 and 1798.82-.84. This law, in effect for over two years, seems to have struck the right balance in this area. Consumers are receiving appropriate and useful notices; and it is our understanding, based upon our consultations with staff of the California Office of Privacy Protection, that the law has not resulted in an unmanageable deluge of notices to consumers. Although anecdotal, the fact that the California statute to a large extent has been followed as a nationwide standard makes it a good indicator of the potential impact of a nationwide bill such as this one.

We also note that the marketplace approach taken by the California statute (as well as the Committee draft) prompts a positive cause-and-effect dynamic. A broad nationwide breach notice requirement will incent companies to improve their practices, thereby, in the long run, resulting in fewer breaches and therefore fewer notices. TRUSTe believes that this generates a much better outcome than setting the initial threshold so high that few breaches generate notice requirements, thereby decreasing the motivation to prioritize security.

MINIMUM REQUIREMENTS FOR A SECURITY POLICY AND STATEMENT

Section 2(a)(1) of the bill would authorize the Federal Trade Commission to promulgate rules requiring companies to implement a "security policy and statement concerning the collection, use, disclosure, and security of personal information." We believe the Committee should consider adopting relevant provisions of the Commission's Security Guidelines for financial institutions provided under Gramm-Leach-Bliley as required components of the security statement provided for in Section 2(a)(1). *Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information,* 16 C.F.R. Part 314. We refer specifically to the following provisions in the *Guidelines:*

§ 314.3 Standards for safeguarding customer information.

(a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

These *Guidelines* provisions reflect a non-prescriptive approach to crafting security policies that we believe is best, given the changing nature of the overall environment, technology and threats.

TRUSTe has particular expertise in the area of drafting sound consumer-facing privacy statements. We believe that the following elements, drawn from guidance set out in recent Federal Trade Commission settlements involving security breaches, should be required of companies' security statements:

1. The kinds of personal information collected and how it is used, disclosed, or otherwise handled in the regular course of business.
2. How consumers can access their information and have it corrected or updated.
3. How company will notify consumers in the event of a security breach, and what redress will be provided to them.
4. Where consumers can learn more about their rights in the event of a breach.

CREATION OF A SAFE HARBOR PROGRAM

As I mentioned earlier, TRUSTe has particular expertise in administering safe harbor programs for industry participants who comply with our guidelines. We recommend that the Committee add to your legislation a safe harbor that (1) allows businesses to comply with a set of guidelines that are approved by the FTC and administered by a third party certification organization; and (2) limits a company's liability, should a breach of security occur, if that company is in full compliance with such guidelines. We believe this is a better approach than simply locking in guidelines through an FTC rulemaking. Through a safe harbor, your legislation could set a floor of protections, and industry self-regulation would then drive even greater levels of protection for consumers, while providing businesses the flexibility they need to develop marketplace solutions to data protection.

CONCLUSION

TRUSTe welcomes this opportunity to share our thoughts on the proposed data protection legislation, and to make the Committee aware of our efforts to serve as the model for industry best practices in information security through our Data Security Guidelines. We look forward to working with the Committee as it continues its efforts to protect the security of personal information in the twenty-first century marketplace.

Mr. STEARNS. And thank you.

Mr. Hintze.

STATEMENT OF MICHAEL HINTZE

Mr. HINTZE. Thank you, Chairman Stearns, Congressman Towns, Chairman Barton, and members of the subcommittee.

My name is Michael Hintze. I am a senior attorney at Microsoft. I want to commend the members of this committee for their attention to data security and identity theft issues. Microsoft shares your concerns.

I also want to thank you for the opportunity to provide our views on the discussion draft. Microsoft firmly believes that now is the appropriate time for Congress to adopt Federal data security legislation. It would be an effective complement to Microsoft's and in-

dustry's efforts to develop technological solutions, to educate consumers, to adopt best practices, and to help enforce existing laws.

Today, I want to highlight some of the key issues raised by the discussion draft.

First, any required information security program should give organizations the discretion to implement the most appropriate technologies and procedures for their respective environments. Microsoft urges the subcommittee to revise the discussion draft to reflect the general framework set forth in the Gramm-Leach-Bliley Act. It should also direct the FTC to allow organizations to adopt the security programs appropriate to their size and complexity, the nature and scope of their activities, and the amount and sensitivity of information that they collect.

Second, any required information security program should apply to all personal information, whether electronic or paper. The consequences of a loss or misuse of personal information on paper can be just as devastating to the affected individual as the loss of that same data in electronic form. Likewise, the programs should not be limited just to sensitive financial information. A single, flexible framework for all information will create a broader protection for consumers and enable companies to comply with one set of security requirements.

Third, a security breach standard should focus on whether the misuse of unencrypted sensitive personal information is reasonably possible. This will ensure that consumers receive notification regarding breaches of information that could lead to identity theft, like Social Security numbers and credit card information with associated passwords. This should also incorporate a materiality threshold like the Federal banking regulators have implied on their guidance on GLB, namely notification is required where there is a reasonable possibility of misuse. Such an approach will prevent notifications from becoming so frequent that consumers disregard them or find themselves unable to differentiate between those that indicate a significant risk and those that do not.

Fourth, different methods of notification should be permitted. The appropriate method for notice will turn on the size and type of entity providing it, the number of people required to receive it, and the relative cost for different methods of providing it. The ways in which an entity typically communicates with its customers should also be considered. For these reasons, the interagency guidance interpreting GLB gives discretion to covered entities to provide notice in any manner designed to ensure that a consumer can reasonably be expected to receive it. Microsoft urges the subcommittee to follow this approach.

Finally, the Federal legislation in this area should create a uniform standard. Security breaches are a national problem, and all consumers should be protected by the same high level of protection. This will also allow responsible businesses to operate without the unnecessary burdens of inconsistent security and notification requirements. For these reasons, we support the preemption provision in the discussion draft. At the same time, we recognize the State Attorney Generals play a vital role in ensuring the companies adhere to sound information security practices. Microsoft therefore

supports any clarification that enables State Attorney Generals to enforce the provisions of this legislation.

Thank you for asking us to share our views on data security legislation and the discussion draft. We are committed to helping create a safe and trusted environment for consumers, and we look forward to working with you and your staff toward this common goal.

[The prepared statement of Michael Hintze follows:]

PREPARED STATEMENT OF MICHAEL HINTZE, SENIOR ATTORNEY, MICROSOFT CORPORATION

Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee: My name is Michael Hintze, and I am a Senior Attorney at Microsoft Corporation. I want to thank you for the opportunity to share with the Subcommittee our views on data security legislation. In light of the number of recent serious security breaches, the increasing concern nationwide over identity theft, and the ever-rising but often inconsistent number of state laws imposing security and customer notification requirements, Microsoft firmly believes that now is an appropriate time for Congress to adopt federal data security legislation.

Microsoft applauds Congress and the members of this Subcommittee for their attention to data security and identity theft issues. As the Federal Trade Commission has reported, in 2003 alone, roughly 10 million Americans suffered from identity theft, costing businesses $47.6 billion and consumers almost $5 billion.[1] As a leading provider of software and online services, Microsoft is particularly concerned that identity theft threatens to erode trust on the Internet, and we are deeply committed to working with you, law enforcement, and others in the industry to maximize deterrence and minimize the opportunities for identity thieves.

Today, I want to address the focus of this hearing—data security legislation. Microsoft generally supports the draft legislation before this Subcommittee, dated June 30, 2005 (the "Discussion Draft"), that would require companies both to adopt an information security program and to notify consumers in the case of a security breach. This legislative approach would be an effective complement to Microsoft's own multi-faceted strategy for protecting individuals' personal information, which includes developing and implementing technological solutions, educating consumers about ways to protect themselves while online, meeting or exceeding industry best practices on privacy and security, and enforcing existing laws. My testimony today highlights some of the key issues raised by federal data security legislation and by the Discussion Draft in particular, and recommends ways to proceed toward the goal of creating a trusted environment for Internet users.

BUSINESSES SHOULD BE REQUIRED TO ADOPT AN INFORMATION SECURITY PROGRAM.

Microsoft supports legislation that would require companies engaged in interstate commerce to adopt an information security program. But in order to be effective, while avoiding unnecessary burdens on responsible businesses, such legislative requirements should be both broadly applicable and sufficiently flexible to meet the security challenges across a wide variety of business environments and scenarios.

(1) *Federal Legislation Should Enable Companies to Implement Security Measures Best Suited for Their Environments.*

First, any such legislative requirement should recognize that security is an ongoing process, that the threats to data security are constantly changing, and that the degree and type of risk can vary from one situation to another. An appropriate and effective information security program will depend on a number of factors, including, but not limited to, an entity's size, the nature of its business, the amount and type of information it collects, and the number of employees that it has. In short, federal legislation must provide flexibility to enable companies to adopt security policies and procedures that are responsive to their risk level.

With this in mind, the framework for an information security program set forth in the Gramm-Leach-Bliley Act ("GLB") is preferable to that outlined in section 2(a) of the Discussion Draft. In GLB, Congress directed the relevant agencies to provide for the establishment of "appropriate . . . administrative, technical, and physical safeguards—

[1] Federal Trade Commission—Identity Theft Survey Report 7 (Sept. 2003), *available at* http://www.consumer.gov/idtheft/stats.html [hereinafter "Identity Theft Survey Report"].

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which would result in substantial harm or inconvenience to any customer."[2]

In response to this directive, the FTC implemented regulations that require the development of information security programs "appropriate to the [subject entity's] size and complexity, nature and scope of . . . activities, and sensitivity of the customer information at issue."[3]

Microsoft believes a flexible framework such as that established by GLB and the FTC's implementing regulations makes sense. It gives individual organizations—which are in the best position to understand the particular security measures that are best suited to the different types and forms of personal information they maintain—the discretion to implement the most appropriate technologies and procedures for their respective environments. In contrast, a set of federally-mandated technical specifications would inevitably impose too high of a burden on some organizations for some information, but not adequately protect some personal information held by other organizations. And, because security measures are constantly changing and improving as technology advances and engineers respond to evolving threats to information security, a one-size-fits-all regime would likely and rapidly become obsolete.[4]

For these reasons, Microsoft urges the Subcommittee to replace its current section 2(a) with language modeled on the framework set forth in GLB and the FTC's implementing regulations. In addition, in light of the importance of ensuring that implementing regulations give companies the discretion to adopt programs that best suit their respective needs, Microsoft encourages Congress to direct the FTC to allow entities to develop information security programs consistent with the following: (1) the entities' size and complexity, (2) the nature and scope of their activities, (3) the sensitivity of the personal information at issue, (4) the current state of the art in administrative, technical, and physical safeguards for protecting information, and (5) the cost of implementing such safeguards. Microsoft believes such a flexible approach is the best way to protect individuals' personal information now and into the future.[5]

(2) *Federal Security Requirements Should Apply to All Personal Information.*

If federal data security legislation includes sufficient flexibility to enable companies to develop security practices and procedures that are tailored to the situation based on these factors, Microsoft believes that federal information security requirements should apply to all personal information housed by an organization in any form, whether electronic or paper. There is no reason to limit the requirements to protect personal information to its electronic form: The consequences of a loss or misuse of personal information in paper form can be just as serious and devastating to the affected individuals as a loss of that same data in electronic form. Likewise, the federal security requirements should not be limited only to sensitive information

---

[2] 15 U.S.C. § 6801(b).

[3] 16 C.F.R. § 314.3.

[4] We also note that as currently drafted, the Discussion Draft could create different regimes for entities that are subject both to GLB and to the reach of new data security legislation. That said, excluding entities covered under GLB from new data security legislation, and then adopting a different standard for other entities, would subject companies that house the exact same information to different regulatory frameworks—e.g., a retailer would be subject to a different information security framework than a bank. For this reason, we support creating uniformity to facilitate both the development of best practices and the development of service-related expertise—such as that provided by auditors—in the area of information security.

[5] This testimony focuses on subsection (a) of Section 2. With respect to subsection (b)—which applies special requirements to information brokers—Microsoft has only two brief observations. First, the definition of "information broker" requires a slight revision to make clear that it applies strictly to those entities whose *primary* business is selling consumer data. Second, while Microsoft generally supports giving individuals access to personal information collected about them, we think that certain reasonable exceptions must accompany such a legislative requirement for it to make sense. For example, access should not be required where the individual requesting access cannot reasonably verify his name or identity as the person to whom the personal information relates; the rights of other persons would be violated; the burden of providing access would be disproportionate to the risk of harm to the individual; revealing the information would compromise proprietary or confidential information, technology, or business processes; or revealing the information would be unlawful or affect litigation or a judicial proceeding in which the business or individual has an interest.

that, if exposed, could lead to identity theft.[6] Although a breach of non-sensitive personal information may not expose individuals to identity theft, it can have other negative consequences.[7] Again, as long as the federal legislation avoids mandating a one-size-fits-all approach to this data and instead provides flexibility, the security requirements can reasonably be applied to all personal information.[8] The creation of such a single, flexible framework for all personal information will create broader protection for consumers as well as increase efficiency for businesses that otherwise could be faced with having to comply with additional and inconsistent security requirements imposed by other state or federal laws.

With this background in mind, Microsoft respectfully suggests that the Subcommittee reconsider the approach taken in section 2(a) of the Discussion Draft. This section appropriately directs the Federal Trade Commission to adopt implementing regulations governing information security programs, but only with respect to a narrow class of sensitive personal information and only with respect to any such information maintained in electronic form. For the reasons stated above, Microsoft urges Congress to expand the scope of this provision.

(3) *Providing Flexibility in the Information Security Requirement is Essential to Avoid Unnecessary Burdens on Small Businesses and Those That Handle Minimal Amounts of Personal Information.*

Finally, we note that a flexible approach to security, such as the one outlined above, also is essential to alleviate the potential burden that a national information security requirement could impose on small businesses. However, if the Committee believes that the potential costs of a national information security requirement necessitates some sort of small business exemption even with the flexible approach that we recommend, Microsoft believes that such an exemption should be triggered by the number of individuals whose personal information an entity handles and not by the size of the business. For example, given the costs of compliance relative to the risks of exposure, it might make sense to exempt from at least section 2(a) an entity that collects, stores, uses or discloses personal information from fewer than 5,000 individuals in any twelve (12) month period.

BUSINESSES SHOULD BE REQUIRED TO NOTIFY CONSUMERS WHEN THERE IS A MATERIAL RISK OF HARM.

Microsoft recognizes that notifying individuals of security breaches can be an effective element in the effort to reduce the costs and other harms associated with identity theft. But we believe that for a notification requirement to provide effective warning to consumers, and to be reasonable and fair for all business entities engaged in interstate commerce, it must be triggered only when there is a material risk of harm to an individual. As recent reports have indicated, an overly broad notification requirement could have negative effects.[9] For example, consumers may begin to receive so many notices that they become accustomed to such notices and/or become unable to differentiate between those breaches that represent a serious risk and those that do not. One likely result is that some consumers will do nothing in response; as a result, the costs of the notice will be incurred in vain, and consumers will continue to bear the risk of any resulting identity theft. Other consumers may err on the side of *over-reaction,* responding to even harmless breaches by imposing credit freezes, fraud alerts or changing or closing accounts—all of which impose significant and unnecessary costs.[10] For these reasons, Congress should proceed carefully when articulating the standard that triggers notification. We believe that the best standard is one that incorporates a materiality threshold like the fed-

[6] By "sensitive information" we mean the kinds of data that is included in the Discussion Draft's definition of "personal information." Although we advocate for a broader scope for security requirements, as we note later, this narrower definition remains relevant for the purposes defining the scope of information that should trigger a notification obligation.

[7] For example, if a number of e-mail addresses wind up in the wrong hands, those individual recipients could be deluged with unwanted spam that renders their e-mail account virtually unusable—or even subjects them to harmful phishing scams that trick them into disclosing sensitive financial information to would-be identity thieves. The exposure of other non-sensitive personal information can have similarly invasive consequences on an individual's privacy.

[8] It is worth noting that the FTC Consent Orders on security have required businesses to implement security programs for all personal information, not just sensitive personal information.

[9] *See, e.g.,* Henry Fountain, "Worry. But Don't Stress Out," Wall Street Journal, June 26, 2005, Section 4, p.1.

[10] *See* Thomas M. Lenard & Paul H. Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches," The Progress & Freedom Foundation 10-11 (July 2005).

eral banking regulators have applied in the Interagency Guidance on GLB—namely, notification is required when there is a reasonable possibility of misuse.

(1) *Notification Obligations Should Be Triggered When Misuse Is Reasonably Possible.*

Microsoft believes that the Interagency Guidance on GLB provides a workable framework for a national notification standard. That guidance focuses on whether, as a result of unauthorized access, "*misuse* of . . . information . . . has occurred or is reasonably possible."[11] Although the Discussion Draft contains a relatively flexible standard, we have some concern that the "may result in identify theft" formulation is vague, and in any event, that the formulation would establish a slightly different standard than GLB has been interpreted to apply to financial institutions. This Interagency standard provides clear guidance to industry and consumers: it appropriately requires an organization to investigate the circumstances of any unauthorized access, and to analyze the risks posed to affected individuals before any notification is required. Microsoft believes it is critical to make companies responsible for determining the details of an unauthorized access to sensitive financial information and the level of threat resulting from the specific circumstances. If an investigation concludes that misuse of a consumer's information has occurred or is reasonably possible in light of the facts surrounding the security breach and the exposure of the information, then notification must be provided. Thus, this standard ensures that only those consumers who are reasonably at risk receive notification, and in so doing, it mitigates against both the risk of over-notification and the risk of consumer over- and under-reaction.

(2) *Notification Obligations Should Cover Only Unencrypted Sensitive Personal Information.*

The purpose of notifying an individual of a security breach is to enable that person to prevent two potential types of identity theft: (1) the misuse of his or her existing credit card or other account, and (2) the fraud that is perpetrated when a thief opens a new account in his or her name.[12] The scope of any notification obligation should be limited to the class of personal information that could lead to such misuse. This information should include Social Security numbers, and it should include credit card information associated with other information that could enable someone to access an account or make a credit card purchase. This information should not include basic personal information—such as name, address or telephone number—that alone or in combination with one another presents virtually no increased risk of identity theft.

The Discussion Draft applies its notification requirements to a narrow class of personal information, which is appropriate. To clarify that this information is particularly sensitive, Microsoft recommends that the Discussion Draft rename this class of information "sensitive financial information." It should then include a broader definition of "personal information" to which the obligations set forth in section 2(a), as described above, apply.

However, within this class of so-called "sensitive financial information," Microsoft believes that encrypted information should be excluded. Data encrypted using standard methods is either impossible or impracticable to decipher. Therefore, there is no reasonable possibility of its misuse if it is accessed without authorization. In addition, by specifically exempting such encrypted information from the standard for notification, Congress will be creating an explicit incentive for companies to adopt encryption technology, thereby reducing the risk of a security breach in the first instance. If Congress has concerns that a general encryption exception is too vague and could be abused,[13] Microsoft would support allowing the exception to apply only to certain levels of encryption—e.g., the encryption level set forth in the Federal Information Processing Standards issued by the National Institute of Standards and Technology—or more generally to encryption adopted by an established standard setting body combined with an appropriate key management mechanism to protect the confidentiality and integrity of associated cryptographic keys in storage or in transit.

---

[11] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736, 15752 (Mar. 29, 2005) (emphasis added) [hereinafter "Interagency Guidance"].

[12] *See* Identity Theft Survey Report, supra note 1, at 4.

[13] We think that, if Congress explicitly exempted encrypted information from the notification requirement, there would be little risk of abuse—after all, as a general matter, it is just as easy to use readily available good encryption technology as it is to use readily available weak encryption technology, so there would be little incentive to use a lower standard.

(3) *Notification Obligations Should Capture Data Maintained In Any Form.*

Microsoft believes that the public policy interest in protecting sensitive financial information against malicious use by third parties extends to all forms of data, regardless of whether it is housed in electronic or paper form. For this reason, we believe the notification requirements set forth in section 3 of the Discussion Draft (like the general security obligations set forth in section 2(a)) should not be limited to electronic or computerized data. This is the approach followed in the Interagency Guidance on GLB.

Although expanding the requirement beyond data in electronic form would potentially heighten the compliance costs associated with this federal legislation, the public policy supports such an expansion. Identity theft can be committed using information obtained offline and in a form other than just computerized data. Simply put, an identity thief can defraud a consumer using sensitive personal information maintained in paper form just as easily as the thief can using computerized data. To adequately protect consumers, the notification requirements of the legislation should therefore apply to all sensitive financial information—regardless of the form in which the information is maintained.

CONGRESS SHOULD GIVE COMPANIES DISCRETION TO DETERMINE THE MOST APPROPRIATE AND EFFECTIVE METHOD FOR NOTIFICATION.

Microsoft believes that for a nationwide notification requirement to be administratively workable, business entities subject to the requirement should have flexibility in how notice is provided. This is because the appropriate method for notice will turn on the size and type of the entity providing the notice, the number of people required to receive notice, the methods by which the entity typically communicates with its customers or other individuals, and the relative costs for different methods of providing notice. For these reasons, the Interagency Guidance on GLB provides discretion to covered entities to provide notice "in any manner designed to ensure that a customer can reasonably be expected to receive [the notice.]" [14]

Microsoft urges Congress to follow the model of the Interagency Guidance by giving companies discretion to issue notice in various ways, so long as the notice is reasonably expected to reach the affected individuals. The Discussion Draft, which would obligate an entity to provide notice to an individual in writing and by email and through the entity's website, is too restrictive, and there is a real risk that it could lead to less effective notifications and/or be too costly for many entities to implement. Rather, federal legislation should enable entities to provide notice via telephone, regular mail, or electronic mail, depending on the circumstance. Indeed, many individuals who have received notices of security breaches report that they appreciate getting them by telephone, which personalizes the process, makes the notice less intimidating, and provides an immediate forum for the individual to ask questions.[15] While telephone notice may not be feasible in cases requiring mass notification, it is an option that should be permissible consistent with the interpretation of GLB.

Microsoft also believes that entities should be required to try to reach individuals directly, unless certain cost or quantity thresholds are present or there is no known number, mailing address, or electronic mail address for an individual. Accordingly, Microsoft would propose using mass media notice and Internet postings only in exceptional circumstances requiring substitute notice.

CONGRESS SHOULD CONSIDER INTERNAL AND LAW ENFORCEMENT INVESTIGATIONS WHEN ANALYZING THE APPROPRIATE TIMELINESS OF NOTIFICATION.

Microsoft is pleased that the Discussion Draft accounts for the immediate obligations of a company in the aftermath of a breach by allowing reasonable time for a company to determine the scope of the breach and to restore any compromised systems before issuing notice of the breach. Microsoft also believes, however, that federal legislation should account for the needs of law enforcement in investigating the breach. It is often the case that immediate notification to the public can interfere with a criminal investigation of the underlying incident. If, for example, law enforcement officials are in the process of identifying or apprehending potential suspects, a public announcement may cause the suspects to flee, destroy evidence, or otherwise obstruct these efforts to bring the perpetrators to justice. The existing GLB guidelines regulating financial institutions, as well as most state breach notification

[14] Interagency Guidance, supra note 11, at 15753.

[15] Larry Ponemon, "Opinion: After a Privacy Breach, How Should You Break the News," Computerworld, July 5, 2005.

laws, have accounted for these concerns by allowing for delayed notification, consistent with the legitimate needs of law enforcement.

The risk of any abuse with this delay in notification is easily addressed by vesting the authority for any such determination in law enforcement, rather than the company itself. As the Interagency Guidance on GLB provides, "notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay." [16] By accounting for these contingencies in imposing a notification requirement, Congress can balance the interests of consumers, the legitimate needs of law enforcement, and the immediate responsibilities of companies suffering data security breaches.

STRONG FEDERAL PREEMPTION IS WARRANTED.

Microsoft believes that for federal legislation to be meaningful in this area, it must address the problem of state laws imposing potentially inconsistent security and notification requirements. In other words, we strongly feel that federal legislation requiring entities to implement an information security program and to notify individuals of security breaches must "occupy the field." As we have seen with the rash of major security breaches over the past several months, information security is a national problem that affects all Americans. Federal legislation that preempts inconsistent state laws is therefore crucial to protect consumers while allowing responsible businesses to operate without unnecessary burdens.

Over the past several months, more than a dozen states have enacted breach notification laws, with a few of these states also requiring entities to adopt security procedures. Although these statutes generally have been patterned after the California law, which pioneered breach-related legislation, the statutes are not uniform, and their differences can be striking. For one, the statutes sometimes differ on the very definition of "personal information," with some states broadly covering any account information, some requiring a name coupled with other identifying information, and some including a Social Security number alone. Similarly, the statutes differ in their jurisdictional scope, with most applying to entities conducting business within the state, but others applying to anyone who possesses information about residents of the state. The statutes are also inconsistent as to when notification is required, with some states providing an exception when the breach is reasonably believed to be harmless. In addition to these disparities, provisions regarding notification period, notification method, and available remedies often vary from state to state.

Although some have argued that the federal provision should create a "floor," above which states are free to impose additional requirements, this would not solve the problem caused by the existing patchwork of state regulation. In such an environment, any company that participates broadly in the national economy must either abide by the strictest applicable standard, or otherwise take measures to compartmentalize its transactions on a state-by-state basis. Under the former approach, any federal legislation would be rendered meaningless absent preemption. And given the realities of today's virtual economy, the latter option is largely impracticable; or, for those companies that tried to comply with requirements on a state-by-state basis, it would potentially cause a harmful distraction from what is important—protecting the security of consumers' personal information and promptly notifying any affected consumers in the event of a security breach that is reasonably possible to lead to the misuse of unencrypted sensitive financial information. Therefore, the only realistic solution that protects consumers while minimizing the operational burdens in responsible businesses is to adopt a nationwide standard for security and notification. That standard should certainly be robust, but, once adopted, should apply uniformly. Hence, any federal legislation on this topic should specifically preempt state security and notification laws.

The Discussion Draft includes an appropriate preemption provision. That said, Microsoft supports adding language to the preemption provision to make clear that only State Attorneys General can bring a civil action under state law that is premised on a violation of the federal legislation. At the same time, we recognize that State Attorneys General can play a vital role in ensuring that companies adhere to sound information security practices. Accordingly, Microsoft also supports any clarification that enables State AGs to directly enforce the provisions of the legislation and also ensures they can continue to rely on their enforcement authority under state consumer protection laws.

---

[16] Interagency Guidance, supra note 11, at 15752.

CONGRESS SHOULD CONSIDER ADDITIONAL PROVISIONS IN DATA SECURITY LEGISLATION.

Requiring entities to implement security procedures that apply to personal information and to notify individuals of security breaches, where the misuse of unencrypted sensitive financial information is reasonably possible, makes sense. But these approaches do not fully address a key concern raised in response to recent security breaches—a lack of transparency as to how companies are using and disclosing personal information in the first place. Individuals want to understand better the entities that maintain their personal information, the types of information they maintain, how they use that information, and the third parties with whom they share such information. For this reason, in addition to supporting reasonable security precautions and notification requirements, Microsoft looks forward to working with the Subcommittee on appropriate legislation that addresses these broader concerns. Microsoft believes that adopting a tailored but more complete approach to data security legislation at the federal level will better inform consumers about who is using their personal information and how, and thereby empower consumers to exercise meaningful control over their personal information both before and after any security breach occurs. In addition, a national standard will give consumers and organizations that are facing a patchwork of privacy and data security requirements at the state level clarity about the standards for collecting, using, disclosing, and storing personal information.

We commend the Subcommittee for holding this hearing today and appreciate your determination to seek strong legislation to help curb identity theft. Thank you for extending us an invitation to share our recommendations on the Discussion Draft, and we look forward to working with you on additional means to help inform and empower consumers both before and after a security breach occurs. Microsoft is committed to creating a trusted environment for Internet users, and looks forward to working with you toward this common goal.

Mr. STEARNS. I thank the gentleman.

Mr. Hoofnagle, welcome.

STATEMENT OF CHRIS JAY HOOFNAGLE

Mr. HOOFNAGLE. Good morning, Chairman Stearns, Ranking Member Towns, and good morning, Chairman Barton.

My name is Chris Hoofnagle. I am senior counsel with the Electronic Privacy Information Center. We are a not-for-profit research center that focuses on privacy founded in 1994 here in Washington. I run the organization's West Coast office in San Francisco.

There are many different consumer protection issues that need the attention in this committee, and we thank you for focusing your attention on privacy and security. Ranking Member Towns, in your introduction, you discussed about how there are new security breaches, it seems, bimonthly. It is actually more than that. The Privacy Rights Clearinghouse has a chronology of data breaches online, and there have been 60 known such breaches since ChoicePoint, the commercial data broker, announced their breach back in February. And when you look at this chronology, you see that it has been a diverse array of businesses. They are in the financial services sector. They are in the retail sector. You also see that there is a diverse number of attackers. There is a diverse number of threats to personal information. Sometimes these breaches are caused by insiders. Sometimes they are caused by outsiders. Sometimes it is just a mistake. And then sometimes it is willful.

So your committee is charged with dealing with a very difficult situation of writing a law that addresses all of these different types of data risks and risks to identity theft and other misuse of information.

With that said, let me focus on just some parts of my testimony.

We were very happy to see the discussion draft. I think it is an important first step in addressing security breach issues. But there are several issues that we wanted to tweak. We have already heard testimony this morning regarding the standard for providing notice. And under this bill, there has to be a risk of identity theft. We really want to emphasize that identity theft is not the only risk to data security.

There have been cases involving stalking. One of the things we work at at EPIC is the problem of investigators who operate online who break security of other companies to get information and sell that information to other people, including stalkers. Data might be accessed by other businesses that are engaged in the attempt to locate people. So, for instance, in New Jersey, there was a major security breach involving 600,000 records at Bank of America and Wachovia. And the people obtaining that information weren't trying to steal anybody's identity. What they were trying to do was sell that data to debt collectors so that the debt collectors could locate them. Data might be accessed for corporate espionage purposes. It might even be access for extortion. There was a case out in California where a hospital had outsourced sensitive medical information to Pakistan. The person in Pakistan handling the data was never paid, and so she took the data and she put it online saying if you don't pay me, I am going to post the rest of this medical data.

And finally, sometimes data is stolen for spam purposes. There was a case here on the east coast where a Time Warner employee was caught with 92 e-mail addresses of AOL subscribers, and he broke the system in order to sell that data for direct marketing purposes.

I also wanted to amplify Ms. Maier's point that it is also very difficult to determine whether or not identity theft is the intent of an attacker and whether or not the attacker is even competent enough to commit that crime. We really need to focus on misuse of data rather than identity theft.

We were also pleased to see that this is a discussion draft on data protection. To us, data protection is an issue that is much broader than security. Data protection includes privacy, the idea that a minimum amount of information should be transferred when entering into a transaction, the idea that people should have access to their information. They should be able to correct it. However, those rights aren't all encompassed in this discussion draft. And we urge you in future drafts to include other privacy rights, because some of the problem here is not just insecurity. The problem is that even if this data were sold securely, there is a problem with the sale that, in some cases, this information should never be sold.

We also emphasize you to include audit trails in the bills. While encryption is a great tool for protecting data from outsiders, encryption does not do a good job when insiders are stealing data and selling it to other people. And it is at that point where audit trails are really important. And what audit trails do essentially is track who accesses data, for what purpose, and whether they disclose it to anyone. And it is the best way to not only deter insiders, but also to catch them once they have broken the security.

I see that I have run out of time, so I want to conclude by saying thank you for holding this hearing and for considering this legislation. And if I can be of help to the committee, please feel free to contact me.

[The prepared statement of Chris Jay Hoofnagle follows:]

PREPARED STATEMENT OF CHRIS JAY HOOFNAGLE, DIRECTOR AND SENIOR COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER WEST COAST OFFICE

INTRODUCTION

Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee, thank you for extending the opportunity to testify on data security legislation.

My name is Chris Hoofnagle and I am Senior Counsel to the Electronic Privacy Information Center, and director of the group's West Coast office, located in San Francisco. Founded in 1994, EPIC is a not-for-profit research center established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC has been on the forefront of the issues being considered in today's hearing. For instance, "commercial data brokers," companies that extract sensitive information from many sources and sell it as a "dossier" to others, have long been a matter of public concern.[1] EPIC has engaged in extensive use of the Freedom of Information Act to determine the extent of interaction between the government and data brokers such as Lexis-Nexis, Acxiom, InfoUSA, and Merlin.[2]

We applaud the Members of the Committee and others who have crafted legislation to address security standards for companies that maintain personal information. In my testimony today, I will provide comment on the Discussion Draft of Data Protection Legislation. The Discussion Draft is a good first step in addressing the security risks presented by companies with personal information, but fails to fully confer upon individuals the tools they need to avoid misuse of personal information. I therefore recommend that the Committee move this legislation, with reasonable enhancements including: an option for credit freeze, a requirement that security measures include audit trails, and public reporting of security breaches to the Federal Trade Commission. I further recommend that the Committee go beyond security issues and consider the privacy risks raised by data brokers.

DATA INSECURITY

Well before the recent news of the Choicepoint debacle became public, EPIC had been pursuing the company and had written to the FTC to express deep concern about its business practices. On December 16, 2004, EPIC urged the Federal Trade Commission to investigate Choicepoint and other data brokers for compliance with the Fair Credit Reporting Act (FCRA), the federal privacy law that helps ensure personal financial information is not used improperly.[3] The EPIC letter said that Choicepoint and its clients had performed an end-run around the FCRA and were selling personal information to law enforcement agencies, private investigators, and businesses without adequate privacy protection.

Since the Choicepoint breach, there has been a steady stream of news articles and public announcements concerning other companies that have failed to secure the personal information of individuals. The Privacy Rights Clearinghouse, a San Diego-based group, has posted a Chronology of these data breaches.[4] As of this writing, this Chronology notes 60 different incidents where a company or government entity reported a security breach involving the Social Security number, drivers license number or financial account number. The Privacy Rights Clearinghouse estimates that 50,000,000 individuals have been affected by these known breaches.

---

[1] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement,* 29 N.C.J. Int'l L. & Com. Reg. 595 (Summer 2004), available at http://www.epic.org/privacy/choicepoint/cp—article.pdf.

[2] EPIC Choicepoint Page, available at http://www.epic.org/privacy/choicepoint/.

[3] Letter from Chris Jay Hoofnagle, Associate Director, EPIC, and Daniel J. Solove, Associate Professor, George Washington University Law School, to Federal Trade Commission, Dec. 16, 2004, available at http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[4] Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, available at http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Jul. 24, 2005).

This Chronology is worth revisiting for at least three reasons. First, it demonstrates the diversity of entities that store sensitive personal information and yet have experienced a security incident. While there have been major security breaches at commercial data brokers such as Lexis-Nexis and Merlin, there have also been security problems at banks, schools, government entities such as motor vehicle administrations, and retailers. This demonstrates the need for intervention across a broad array of entities.

A privacy-friendly approach would first emphasize the need for reducing the amount of personal information collected and maintained. Where retention of personal information is necessary, these entities should be subject to a framework of "Fair Information Practices." Fair Information Practices, or "FIPs," constitute a framework of rights and responsibilities that require entities to minimize the amount of information they collect, to use it only for purposes specified by the individual, to hold it in a secure manner, and to provide the individual access to and of the ability to correct their personal data.

Second, the Chronology demonstrates that security breaches may occur for reasons other than to commit identity theft. For instance, insiders at Bank of America, Wachovia, PNC Bank and Commerce Bank sold customers' personal information to attorneys and others who were engaged in debt collection efforts.[5] That breach affected the records of over 600,000 accountholders. Sometimes systems are compromised for voyeuristic purposes, such as obtaining the contact information or communications data of celebrities or law enforcement officials.[6] Security breaches may be motivated by a company attempting to obtain information about a competitor. Finally, extortion may motivate someone to obtain and disclose an individual's personal information. For instance, in 2003, a Pakistani clerical worker performing transcription services for an American hospital threatened to release medical records if she was not paid for her services.[7] Accordingly, Congress' approach should recognize that identity theft is not the only harm to be avoided. Legislation passed by Congress should recognize that security breaches may be motivated by a number of crimes unrelated to attempted identity theft.

Third, the Chronology demonstrates that entities that maintain personal information are subject to many different security risks. While we typically think of outsiders, such as malicious computer hackers, as the prime security risk, the Chronology shows that dishonest employees are a major security problem. Accordingly, Congress' approach should include measures likely to catch insiders who sell information. Audit trails—a requirement that entities record who accesses and discloses personal information—would go far in deterring and detecting dishonest insiders.

THE DRAFT SHOULD CONTAIN CREDIT FREEZE LANGUAGE

In the Senate, Members are considering legislation that will prevent identity theft by allowing individuals to "freeze" their credit. Under these proposals, individuals can opt to erect a strong shield against identity theft by preventing the release of their credit report to certain businesses. Because a credit report is always pulled before a business issues a new line of credit, a freeze will make it very difficult for an impostor to obtain credit in the name of another person.[8]

According to US PIRG, 10 states have credit freeze laws enacted.[9] The New Jersey law offers consumers the most benefit—any resident may freeze their credit report at minimal cost, and consumer reporting agencies must make the thaw mechanism work quickly, so that individuals can take advantage of instant credit offers.

We believe that a credit freeze is a good approach that will minimize security risks and reduce the risk of identity theft. Simply stated, this provision will make it more difficult for others to use a consumer's credit report without their consent. Consumers will always have the ability to provide their credit reports in those transactions that they initiate.

---

[5] Jonathan Krim, *Banks Alert Customers of Data Theft,* Washington Post, May 26, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/05/25/AR2005052501777.html

[6] Kelly Martin, *Hacker breaches T-Mobile systems, reads US Secret Service email and downloads candid shots of celebrities,* SecurityFocus, Jan. 12, 2005

[7] David Lazarus, *A tough lesson on medical privacy Pakistani transcriber threatens UCSF over back pay,* Oct. 22, 2003, available at http://www.sfgate.com/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL.

[8] Chris Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors,* Securing Privacy in the Internet Age, Stanford University Press (forthcoming 2006) available at http://ssrn.com/abstract=650162

[9] US PIRG, State Breach and Freeze Laws, available at http://www.pirg.org/consumer/credit/statelaws.htm.

THE NEED TO CONSIDER GENERAL PRIVACY PROTECTIONS

The Discussion Draft would establish important security safeguards for all businesses with personal information, and heightened duties on information brokers. But while the Discussion Draft addresses security concerns, it does not contemplate whether general privacy restrictions are appropriate.

Information brokers have operated under a self-regulatory schema, known as the Individual Reference Service Group ("IRSG") Principles. Through these principles, the industry conferred upon itself the authority to sell detailed dossiers to almost anyone for almost any purpose. It was the promiscuity of these principles that led to the most recent Choicepoint breach, because the principles allowed data brokers to choose who is "qualified" buyer of personal information, and allowed sale to anyone with a "legitimate" business purpose.

A serious inquiry should be made into the purposes for which these dossiers are being sold. Congress should set limits on the contexts in which personal information can be sold, and when data is sold, limit the secondary uses of personal information.

THE DISCUSSION DRAFT OF DATA PROTECTION LEGISLATION

Section 2 Requirements for Information Security: All Companies

This section directs the Federal Trade Commission ("Commission") to promulgate regulations to require companies to implement policies and procedures to protect personal information. Companies would have to develop a security policy and statement on use of personal information. Companies would have to identify an employee as being responsible for information security. Finally, companies would have to develop processes to take preventive and corrective action to address security vulnerabilities, including the use of encryption.

We applaud the Members for encouraging the use of encryption to protect personal information. However, we wish to emphasize that once data is encrypted, it may still be vulnerable. For instance, the company may choose a poor encryption method that can be decoded easily. There is also the risk that a malicious actor, especially when he is an insider, will have the key or password to decode the encryption. Accordingly, an entity that uses encryption should not automatically be exempt from other data security responsibilities, such as the requirement to provide security breach notices.

We suggest three improvements to this section:

First, this section could be significantly enhanced by a requirement that companies employ audit trails to deter and detect insider misuse of personal information. An audit trail would record who accessed individuals' information, the purposes for which it was accessed, whether it was disclosed, and to whom it was disclosed. Simply put, encryption will be most effective at protecting data from outsiders; auditing will be a strong deterrent to insiders.

Second, where possible, companies should require customers to establish a password system for access to their file. Currently, many entities with sensitive personal information will give access to files based on the provision of simple biographical information, such as billing address, phone number, date of birth, or Social Security number. The problem is that these biographical identifiers often are found in publicly-available databases, such as phone books, public records, or the Internet.

Passwords have some disadvantages. Sometimes people choose poor passwords, but an institution can correct this by requiring the password to be a certain length. Sometimes individuals forget passwords, and in cases where that is a concern, a "shared secrets" password system could be employed. In such a system, the customer and business agrees upon a series of questions that can be asked to verify identity. They could include asking the customer what street they lived on as a child, the name of their first pet, or their favorite book or sports team. The questions are periodically rotated to prevent an impostor from learning these secrets.

Third, some companies are using automatic number identification ("ANI"), a form of caller ID, to identify or authenticate customers. ANI offers additional security over caller ID, but it now appears that ANI too can easily be "spoofed," or falsified, through the use of VOIP telephony.

In crafting security guidelines, the Commission will have to consider that new technologies may pose new risks to security systems. Accordingly, we recommend that the Commission be directed to periodically review security requirements, and new threats to personal data.

Section 2 Requirements for Information Security: Special Requirements for Data Brokers

This section would require information brokers to be audited by the Commission. It would also require data brokers to allow individuals to obtain their dossier annually at no cost.

We applaud these requirements. Individuals should be able to obtain personal information held by data brokers at no charge. Currently, industry practice on providing individuals access to their personal information varies widely. For instance, it is not clear whether information brokers provide the complete file of personal information when an individual makes a request for access. Choicepoint provides free access, and in a recent study where 11 people requested their files, the company provided individuals with their dossiers in a timely fashion. However, the study showed the many errors were found in the Choicepoint dossiers.[10] Acxiom charges $20 for access, but in the study, the company only fulfilled half of the requests made and took an average of 89 days to comply. A legal mandate for free and timely access is needed.

Section 3 Notification of Database Security Breach

This section specifies the instances when a company must disclose to individuals that their personal information has been obtained by an unauthorized person. It defines breach of security as "the compromise of the security, confidentiality, or integrity of data that results in, or there is a reasonable basis to conclude has resulted in, the acquisition of personal information by an unauthorized person that may result in identity theft." It specifies how a company must give notice, and what the notice must contain. It specifies that a company with a security breach must provide three credit reports and a year of credit monitoring service to victims.

There are several critical aspects to this portion of the legislation. First, of course, is the severity of events that constitute a "breach of security." The language in the Discussion Draft tracks the California standard, except that the Discussion Draft includes the requirement that the security breach "may result in identity theft."

As we explained above, identity theft is only one risk from unauthorized access to personal information. Unauthorized access may be gained for other purposes that cause harm to the individual, such as stalking, obtaining information for debt collectors, corporate espionage, extortion, or mere voyeurism. The purpose of data security breach legislation is not just to warn individuals of a risk of identity theft; it is also designed to shine a light on poor data practices.

More importantly, as identity theft expert Beth Givens has argued, companies often cannot tell whether a security breach may result in identity theft. The motives of a person who gained access are not always clear. Identity theft can also occur months or even years after a security breach.

There has been much discussion of whether to give companies discretion to determine whether notice to the public is justified. No such discretion is given by the California law, and Congress should carefully consider the consequences of extending discretion at the federal level. It is already the case that one information broker, Acxiom, engaged in acrobatics to avoid giving notice of a 2003 security breach that reportedly involved 20 million records.[11]

Because it is difficult to gauge the risk of identity theft, because there are harms other than identity theft which may result from security breaches, and because there is already evidence that companies will go to great lengths to avoid giving security breach notices, we recommend eliminating the language that gives companies discretion not to give notice based on a determination whether the breach "may result in identity theft."

If Congress chooses to give some measure of discretion, it should set a standard that requires notice where there is a "reasonable risk or reasonable basis to believe that such access could lead to misuse of personal information." This standard recognizes that security breaches should focus on "misuse" of personal information instead of just identity theft, and would allow companies not to give notice where there is no reasonable risk of harm. There should also be a duty to thoroughly investigate suspected breaches. The standard set should not give data holders incentives to ignore these incidents.

---

[10] PrivacyActivism, *Data Aggregators: A Study of Data Quality and Responsiveness,* May 18, 2005, available at http://www.privacyactivism.org/Item/222.

[11] Robert O' Harrow, Jr., No Place to Hide 71-72, Free Press (2005). DOJ, *Milford Man Pleads Guilty to Hacking Intrusion and Theft of Data Cost Company $5.8 Million,* Dec. 18, 2003, available at http://www.usdoj.gov/criminal/cybercrime/baasPlea.htm; DOJ, *Florida Man Charged with Breaking Into Acxiom Computer Records,* Jul. 21, 2004, available at http://www.usdoj.gov/opa/pr/2004/July/04__crm__501.htm.

The second critical factor is the scope of businesses that will be subject to the notification requirement. We think the standard set forth by the bill—any company that owns or possesses data—is the appropriate one. The California standard—any company that owns or licenses data—misses the mark in that some companies merely process data for others, but may still experience a breach.

A third critical factor is the form of notice. The California security notice legislation was in effect a type of "Freedom of Information Act" for security standards. Consumers and policymakers have benefited from learning more about security standards and breaches, but there have also been significant limitations—in many cases, only the victims learn of the breach. Consumers and policymakers would benefit from hearing of all breaches through a website that could be operated by the Commission. We would recommend that the following language be added to the legislation, so that there will be public reporting of security breaches:

> "Information submitted to the Commission under sections 2(b)(1) and 3(a)(2) shall be posted at a publicly available website operated by the Commission."

Section 4 Enforcement by the Federal Trade Commission

This section specifies that the Commission will enforce the law, under its authority to address unfair and deceptive trade practices.

We recommend adding enforcement powers so that state Attorneys General can also enforce the law.

We further recommend that the Commission's authorization and appropriation be increased to account for the burdens associated with enforcing this law. The Commission must oversee a plethora of business practices—from deception in funeral businesses to "power output claims for amplifiers utilized in home entertainment products."[12] This wide range of responsibility requires adequate funding.

Section 5 Definitions

This section defines the many terms in the legislation, including identity theft and information broker.

The definition of "identity theft" is narrow and does not encompass the full range of activities normally understood as identity theft. The current definition focuses on the use of others' personal information for the purpose of engaging in "commercial transactions." This does not recognize the problem of "criminal identity theft," where an individual uses the personal information of another in his interactions with law enforcement, leaving the victim with a criminal record. Accordingly, we recommend that if the law continues to include this term, that it be broadened to recognize other activities commonly understood to be "identity theft."

Defining "information broker" is a challenge. Many companies are engaged in the transmission of personal information to third parties. In some cases, this occurs within the individual's expectation, such as when information must be transferred to execute a transaction requested by a consumer. In others, the transfer of personal information raises unique privacy risks, and such businesses should be included in the definition of "information broker."

Further complicating this matter is the qualifier "whose business is to collect, assemble, or maintain personal information." Information brokerage is just a small percentage of the business of a company like Lexis-Nexis or even Choicepoint. Lexis-Nexis is a huge company; most of its information products have no bearing on privacy, such as the company's legal and scholarly research databases. According to Choicepoint, only about 11% of its operations consist of information brokerage outside the Fair Credit Reporting Act. Can it be said that Lexis-Nexis and Choicepoint are entities "whose business is to collect, assemble, or maintain personal information" for provision to third parties?

There have been many attempts to define an information broker, and thus far, we think the best is contained in S. 1332:

> The term 'data broker' means a business entity which for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of collecting, transmitting, or otherwise providing personally identifiable information on a nationwide basis on more than 5,000 individuals who are not the customers or employees of the business entity or affiliate.

This definition limits the scope of the law to companies that regularly engage in maintaining large databases on non-customers for the purpose of providing them to a third party. It provides a good starting point for further discussion.

Congress should also consider giving the Commission rulemaking authority to address circumvention of this definition through corporate restructuring or techno-

---

[12] *See generally* Title 16 of the Code of Federal Regulations, available at http://www.access.gpo.gov/nara/cfr/waisidx_05/16cfrv1_05.html.

logical tweaks. In passing the Fair and Accurate Credit Transactions Act, Congress included a provision that prohibits "technological circumvention" of the Fair Credit Reporting Act's provisions. The concern was that through database design or corporate reorganization, a consumer reporting agency may escape obligations to provide a free credit report. We think that a similar provision would be appropriate her to avoid a situation where a company simply reorganized to avoid security or privacy responsibilities.

The definition of "personal information" in the Discussion Draft is narrower than the California law. Under the California law, personal information "means an individual's first name or first initial and last name in combination with . . ." a Social Security number, drivers license number, or account number. The Discussion Draft would require the individual's first and last name, instead of just the first initial. We think that the federal legislation should be as broad as the California definition in this regard.

We further recommend that section 5(5)(A)(iii) should be modified. That section treats an account number in combination with an access code as "personal information." As currently written, it gives credit card companies an out from giving notice by claiming that the three-digit security code on the card must be present for a breach to occur. That is, even though the three-digit code is not necessary to make charges, they will claim that a breach does not require notice unless that code is included in the compromised files. We accordingly recommend that this section be changed to:

> "(iii) Financial account number, or a credit card number, or a debit card number in combination with any required security code."

Section 6 Effect on Other Laws

This section specifies that all state laws concerning breaches of security or notification to individuals of breaches of security would be preempted.

The preemption language in the Discussion Draft is overly broad; it risks unintentionally preempting many different state laws that address security, but are not the target of this law. Data security needs are too varied to accommodate a nationwide uniform standard. Floor preemption is more appropriate here.

In privacy and consumer protection law, federal ceiling preemption is an aberration. Historically, federal privacy laws have not preempted stronger state protections or enforcement efforts. Federal consumer protection and privacy laws, as a general matter, operate as regulatory baselines and do not prevent states from enacting and enforcing stronger state statutes. The Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Driver's Privacy Protection Act, and the Gramm-Leach-Bliley Act all allow states to craft protections that exceed federal law.[13] Even the Fair Credit Reporting Act is largely not preemptive.[14]

Although the federal government has enacted privacy laws, most privacy legislation in the United States is enacted at the state level. Many states have privacy legislation on employment privacy (drug testing, background checks, employment records), Social Security Numbers, video rental data, credit reporting, cable television records, arrest and conviction records, student records, tax records, wiretapping, video surveillance, identity theft, library records, financial records, insurance records, privileges (relationships between individuals that entitle their communications to privacy), and medical records.[15]

Finally, the data industry is in a weak position to argue that it cannot comply with state laws. This is an industry that "segments" or groups people by characteristics at the zip+4 level. They know where you live now, and where you lived ten years ago. No other industry is better equipped to use technology to comply with state law than the data brokers.

Section 7 Effective Date and Sunset

This section specifies that the act will take effect a year after enactment, and sunset 10 years from enactment.

While Congress and the Commission should continue to revisit data security issues, security requirements and rights in personal information should not automatically sunset. We suggest striking the sunset provision.

---

[13] Respectively at 18 U.S.C. § 2510 et. seq., 12 U.S.C § 3401, 47 USC § 551(g), 18 USC § 2710(f), 29 USC § 2009, 47 USC § 227(e), 18 U.S.C. § 2721, and Pub. L. No. 106-102, §§507, 524 (1999).

[14] *See* 15 USC § 1681t.

[15] See generally, Robert Ellis Smith, Compilation of State and Federal Privacy Laws (Privacy Journal 2002).

Section 8 Authorization of Appropriations

This section would authorize a yet to be determined amount to the Commission. For reasons explained above, we support greater funding of the Commission.

CONCLUSION

Mr. Chairman and Members of the Committee, thank you for inviting me to on the Discussion Draft of Data Protection Legislation. The Discussion Draft is a good first step in addressing security risks presented both by ordinary companies and information brokers. We recommend that the Committee move the legislation, with reasonable enhancements, including an option for credit freeze, requirements that security measures include audit trails, and public reporting of security breaches to the Federal Trade Commission.

Mr. STEARNS. Thank you.

Mr. Burton, welcome.

STATEMENT OF DANIEL BURTON

Mr. BURTON. Thank you, Chairman Stearns, Congressman Towns, distinguished members of the committee. My name is Daniel Burton. I am Vice President of Entrust, Inc., which is headquartered in Addison, Texas. And Entrust is proud to secure the digital identities and information of over 1,400 government agencies and enterprises and over 50 countries around the world.

Let me start by underscoring two points. First, the data security threat you address today is very real, and your efforts are timely and critically needed.

Second, there are effective market solutions readily available that can address most of today's threats and give your constituents greater peace of mind.

Over the past few years, while the public's attention has been riveted on homeland security, old-fashioned crime has infiltrated the Internet. The terms we use to describe it: spyware, phishing, identity theft, were relatively unknown only a few years ago. These cybercrimes occur at the crossroads of privacy and security and are prevalent today.

This committee's draft bill correctly embodies two critical principles necessary to combat cybercrime.

First, it encourages enterprises to implement effective data protection programs to prevent the theft of digital information. Second, it encourages them to alert individuals when their personal information has been compromised.

Since I last testified before this committee just 2 short months ago, 17 new data breaches have been made public. They cover a broad cross-section of organization, from a big data services company to a high school. In the aggregate, these notifications indicate that over 44 million identities may have been compromised in just the past 78 days. And these are just the breaches we know about.

In response, 18 States, most of which are represented by distinguished members on this committee, have passed breach notification laws. In addition, we have seen private class action lawsuits, State lawsuits, shareholder lawsuits, an FTC enforcement action, and a major corporation assert that it will no longer tolerate lax data security from business partners.

The fact is, many entities who hold sensitive personal data simply do not keep it safe, either by choice or because they do not understand how to protect it. If they are left to figure it out on their own without any guidance from Congress, many of them will con-

tinue to lose the battle against today's sophisticated cybercriminals, and your constituents will pay the price.

Clearly, it is time for Congress to act. This committee's draft bill is an essential step in the right direction, and Entrust is proud to support it. This draft gets a lot of the key elements right. It focuses on electronic data. It covers all persons who hold personal data, and includes special requirements for data brokers. It encourages comprehensive information security policies and procedures. It establishes a national breach notification requirement that preempts State law. It gives regulatory authority to the Federal Trade Commission. It points to a reasonable notification standard. The committee is to be commended for including these elements in the draft bill.

Given Entrust's experience, I would recommend three other critically important additions to make sure that this bill accomplishes what you want it to.

No. 1, you must actively engage corporate executive management and boards of directors in the effort to secure sensitive digital information. Specifically, the bill should require regular information security risk assessments, audits, and progress reports to CEOs and boards of directors. These measures will assure that American board rooms begin to view information security as a key component of business plans, not just another burdensome technology issue.

No. 2, just like the 18 States that have passed breach notification laws, you should create a safe harbor for companies who do the right thing and encrypt their data. All of the State breach notification laws that have been passed so far require consumer notification only in the event of a breach of unencrypted personal information. The reason is that even if thieves get access to encrypted data, they will not be able to make sense of it since it consists of an indecipherable jumble of symbols to anyone looking at it without the proper keys. If the members of this committee are going to preempt their own State laws, I would strongly encourage you to embrace their wisdom on this issue.

Third, and finally, in order to create a safe harbor for strong encryption, you must define it. To assure that you define strong encryption without picking winners and losers or locking in a static technology, you should reference NIST's standards. NIST's standards are developed in close consultation with industry and are flexible enough to allow standards bodies to drop older encryption products and certify new ones as the technology evolves. Failure to define encryption in Federal legislation could lead to the emergence of conflicting requirements across the United States.

In closing, I want to reaffirm that your draft data security bill makes a strong legislated statement. These additions will help make sure that it fully accomplishes your purposes of protecting sensitive personal information.

Thank you.

[The prepared statement of Daniel Burton follows:]

PREPARED STATEMENT OF DANIEL BURTON, VICE PRESIDENT OF GOVERNMENT AFFAIRS, ENTRUST, INC.

Good Morning. Chairman Stearns, Ranking Member Schakowsky and distinguished Members of the Subcommittee, thank you for holding this hearing and giving me the opportunity to provide testimony on this important subject. My name

is Daniel Burton, and I am Vice President of Government Affairs for Entrust, Inc. We are headquartered in Addison, Texas and are proud to provide cybersecurity software solutions for over 1,400 government agencies and enterprises in more than 50 countries. In my testimony today, I will discuss data security and this Committee's draft legislation.

As a global leader in securing digital identities and information, Entrust has insight into the severity of the risks and the nature of the threats that concern consumers, enterprises and policymakers alike. Our extensive international experience securing governments and enterprises around the globe, along with our policy experience co-chairing two national information security task forces, leads me to underscore two points. First, the threat you attempt to address today is very real and your efforts are timely and critically needed. Second, there are ready and effective market solutions available that can address most of today's threats, secure many of our most vulnerable digital assets and, more importantly, give your constituents a greater peace of mind.

Over the past several years, while the public's attention has been riveted on homeland security, old fashioned crime has infiltrated the Internet. The terms we use to describe it—spyware, phishing and identity theft—were relatively unknown only a few years ago. These crimes occur at the cross-roads of privacy and security. Most of them involve gaining unauthorized access to sensitive personal data. Sometimes criminals gain this access through technological means; sometimes they trick users into revealing the data; sometimes they rely on insiders with privileged access; and sometimes they hack into data bases or steal the information outright. No matter how the crime is committed, however, the goal of public policy remains the same—encouraging enterprises to implement effective data protection programs to prevent theft and to alert individuals when their personal information has been compromised. This Committee's draft bill correctly embodies these two important principles.

Since I last testified before this committee two months ago, seventeen new data breaches have been made public. They cover a broad cross-section of organizations—data services companies, banks, corporations, universities, a high school, a community college and a travel agency. In the aggregate, these notifications indicate that over 44,600,000 identities may have been compromised since May of 2005. And these are just the breaches we know about. Many breaches are uncovered deep inside an organization, never brought to the attention of senior management and therefore never made public. Others, as we have learned from some recent announcements, tend to be minimized in initial public statements and only fully disclosed later under scrutiny. As the legal and market penalties for these breaches mount, organizations will be even more careful about what they reveal.

In reaction to data breaches, 35 states have introduced data breach legislation, and 18 states have passed breach notification laws. The specifics of these laws vary from state to state, but they all require organizations to notify individuals whose personal information has been compromised. In doing so, they aim not only to protect consumers, but also to encourage organizations to be more diligent in securing personal information. In the absence of Federal legislation, we're sure to see even more states pass data breach notification bills next year.

State legislatures are not alone in responding to these breaches. In the past few months, we have seen private class action lawsuits, state lawsuits and shareholder lawsuits against organizations that have suffered breaches. As more and more breaches are made public, more lawsuits are sure to be filed. In addition, Federal regulators have engaged. The FTC recently settled an enforcement action against BJ's Wholesale Club that requires it to implement a comprehensive security program and undergo independent audits. Perhaps most importantly, the recent announcement of VISA that it may no longer do business with CardSystems Solutions, Inc., is a clear market signal that business partners will no longer tolerate lax data security.

The public avalanche of data breaches is damaging consumer confidence and could endanger our economy. A January 2005 IDC Survey showed that close to 60% of US consumers are concerned about identity theft. A recent survey that Entrust conducted reaffirmed this concern. It found that 80% of individuals are worried about someone stealing their on-line identity and using it to access their on-line bank accounts. If consumers pull back from online transactions, the promise of e-commerce and the productivity gains of the past decade will be at risk.

We should remember that it's no longer just your local bank and credit card company that hold your personal information. Numerous retailers, data brokers, on-line merchants, corporations and other vendors also have ready access to it. Many of these entities do not take adequate measures to keep this information safe, either by choice or simply because they do not understand how to protect it in a world of

constantly evolving digital threats. If they are left to figure it out on their own, many of them will continue to lose the battle against today's sophisticated cybercriminals. In fact, things may get worse before they get better because even when organizations do grasp the need for comprehensive data security, it still takes time to put effective programs in place. This delay is unfortunate because there are ready and effective solutions available to address most of today's threats.

Given the substantial risks facing American consumers and the US economy, it is time for Congress to act. In doing so, it should take into account the needs of consumers, corporations and citizens, and embrace the protections embodied in the 18 state breach notification laws. Congress should encourage a program of security management that balances the need to protect personal information and notify consumers in the event of a breach with the need to grow the digital economy and encourage innovative technology solutions. This Committee's draft data security bill is an essential step in the right direction, and Entrust is proud to support it.

This draft bill gets a lot of the key elements right:

- **It focuses on electronic data.** The bill correctly recognizes that the crux of the problem is the growing theft of computerized data. As you know, the electronic data targeted by cyber criminals contains the personal information that has become such a valuable commodity in today's world. Your draft bill, by resisting the temptation to create an overly expansive approach to data security that includes both paper and electronic records, strikes to very core of what must be protected.
- **It covers all persons who hold personal data and includes special requirements for data brokers.** Breach notification should apply to any agency, enterprise or person who owns or licenses computerized data containing the sensitive personal information of others. It should not be limited to data brokers. The goal should be to protect sensitive personal data, no matter who holds it, instead of focusing exclusively on a few specific sectors or industries.
- **It encourages comprehensive information policies and procedures.** This is a vital provision that is not yet included in many state breach notification bills. Reasonable security practices encompass a combination of technology, policy and management expertise. Organizations that own or license computerized data containing personal information should be required to develop, implement and maintain reasonable security measures based on widely accepted voluntary industry standards or existing Federal law.
- **It establishes a national breach notification requirement that pre-empts state law.** Since 18 states have already passed data breach notification laws and more are sure to do so, it is incumbent on Congress to create a consistent national standard.
- **It gives regulatory authority to the Federal Trade Commission (FTC).** Given the reality of widespread cyber crime and the fact that market forces have not resulted in adequate data security programs, it is appropriate for Congress to provide regulatory guidance. The FTC is the proper regulatory agency to undertake this responsibility.
- **It points to a reasonable notification standard.** The goal of legislation should be to make the notification standard as narrow yet as effective as possible in order to encourage notice of breaches that carry a significant risk and discourage over-notification. In crafting this trigger, Congress should bear in mind that in most cases it is difficult to determine what happens to the data after it is breached and therefore to calibrate precisely the risk to consumers.

The inclusion of these important elements in the Draft Bill is to be commended. Given Entrust's experience, I would encourage this Committee to include three additional changes to the bill in the hope of further improving its efficacy and cost efficiency. These changes will appeal to governments, businesses and other entities that control critical data since they will help provide a meaningful road map to navigate the tricky and technical world of data management.

1. Require the Active Engagement of Executive Management—Whether Congress gives the FTC responsibility for providing regulatory guidance for reasonable security or leaves that responsibility with industry, it is imperative that corporate executive management and boards of directors be actively engaged. American board rooms must begin to view information security as a key component of business plans, not just another burdensome technology issue. Congress must realize that securing digital information is not simply a technical challenge, but one that begins with management embracing its responsibility to protect data in the first place. While it is essential to encourage such technologies as strong authentication and encryption, they cannot substitute for executive attention and corporate policy. In this respect, the draft bill's focus on appropriate policies and procedures is critical. Specifically, the bill should require regular risk assessments, audits, and

progress reports to the CEO and Board of Directors. These types of actions will go a long way toward elevating information security in the corporate decision-making process.

2. Create an exemption for Encryption—The Committee's bill should also encourage the use of strong encryption, just as California and other states have done. All of the 18 state breach notification laws that have been passed so far (Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, North Dakota, Rhode Island, Tennessee, Texas and Washington) require consumer notification only in the event of a breach of *unencrypted* personal information.

The reason for this exemption is that even if thieves get access to encrypted data, they will not be able to make sense of it. Encrypted data consists of an undecipherable jumble of symbols to anyone looking at it without the proper keys. This provision is especially important for laptops and disks that are lost or stolen in transit. I should note that state legislatures included this exemption not because of any lobbying by the high tech industry, but because of the requests of organizations that hold significant amounts of personal data. These organizations view this technology as the final line of protection to ensure that even if criminals get past the gate they cannot access the real content. This provision also helps provide guidance to organizations that want to secure their digital information but are unsure what baseline measures to take.

3. Define Encryption—In order to define encryption without picking winners and losers or locking in a static technology, Congress should reference NIST standards. I would recommend the following definition for encryption, which has been adopted by the Cyber Security Industry Alliance:

> *The protection of data in storage or in transit using an approved encryption algorithm implemented within a validated cryptographic module that has been approved by NIST or another recognized standards body, combined with the appropriate key management mechanism to protect the confidentiality and integrity of associated cryptographic keys in storage or in transit.*

This definition references standards that are developed in close consultation with industry, and does so in a flexible way that allows standards bodies to drop older encryption products and certify new ones as the technology evolves. It is important to note that it also requires that the cryptographic keys which can unlock this data be managed in an appropriate, secure manner since these keys are just as valuable and sensitive as the data they protect. The flexibility this definition allows is crucial since any definition that cannot accommodate evolving technology cannot help defend against evolving threats. Because this definition is not vendor or product specific, it will allow the market to drive choices about security solutions. Failure to include a definition in Federal legislation could lead to the emergence of conflicting encryption requirements across the United States.

This Committee's draft Data Security Bill makes a strong legislative statement. These additional suggestions will better protect data, harmonize the Federal plan with laws that have been adopted by 18 states, and help show organizations how to secure the personal information in their possession. By including language that encourages organizations to consider information security at the highest levels of management, Congress can encourage appropriate data security practices at all levels of an organization. And by including language that encourages the use of encryption and defines it, Congress can create a formidable second line of defense against thieves and hackers.

The stage is set for Federal legislation. The menace of cyber crime is undeniable. The cost to consumers and enterprises is enormous. And the multiplicity of state bills highlights the need for a consistent Federal regulatory framework. This draft bill gets a lot of the key elements right and provides an excellent platform for legislation. This Committee should be congratulated for its leadership.

Mr. STEARNS. Thank you, Mr. Burton.

I will start with the questions.

Mr. Hoofnagle, I think you read about these security breaches and its great headlines. And I guess of the 60 different breaches, 50 million American consumers have been affected. I think you mentioned that in your testimony. Do you know how many individuals were either victims of identity theft or information that was misused within this huge number?

Mr. HOOFNAGLE. Mr. Chairman, that is a very difficult issue to determine.

Mr. STEARNS. Yes.

Mr. HOOFNAGLE. In reference to the ChoicePoint breach where reportedly 144,000 records were stolen by a fraud ring, a Nigerian fraud ring in California, 750 of those cases have been associated, in some way, with identity theft. But it is very difficult to track down when or if identity theft occurs. There is also the difficulty that there might be major delay between the data security breach and the actual crime of identity theft since critical identifiers used by credit companies, such as your Social Security number and date of birth, do not change, if it is stolen today, there is really no reason why someone can't victimize you 2 years down the road.

Mr. STEARNS. You know, I read these in the newspaper, and you know, it is just so alarming. But as you point out, a very small number of that are affected by this identity theft. You testify that security breaches can occur for reasons other than identity theft, and so I mean, do we want to come back with this bill and put this overlay of the Federal Government on these people when we are trying to really pinhole a problem here? Should the bill require notification for risk of these other misuses?

Mr. HOOFNAGLE. I think the Federal banking standards are set at reasonable risk of misuse of personal information, and I think misuse is the right term to use rather than identity theft. For instance, in this New Jersey case where bank officials were selling data to debt collectors, it did not involve——

Mr. STEARNS. Identity theft, right.

Mr. HOOFNAGLE. It did not involve identity theft. This was a case where, you know, the security was being breached for profit at these sophisticated financial institutions. It didn't have anything to do with identity theft. It had to do with this other type of privacy violation. And I think that the legislation should encompass that type of security breach.

Mr. STEARNS. Mr. Hintze, you state in your testimony that legislation should codify into law the FTC implementing regulations under the Gramm-Leach-Bliley. Should the FTC be given the authority to modify these provisions by rule to adapt to changing business and security concerns? Why or why not?

Mr. HINTZE. Yes, Mr. Chairman. We think that the FTC should have the authority to make rules in this space, however that authority should be guided by Congress in terms of directing the FTC to adopt a flexible standard around information security programs.

Mr. STEARNS. If the notification obligations are only applied to encrypted data, might that let some potential bad actors off the hook? Why or why not?

Mr. HINTZE. We don't think so. We think the standard around unencrypted data is a reasonable standard. It is the standard that the States have adopted. There have been questions raised about how you define encryption, and while we wouldn't support a specific mandate in the legislation itself, we could support something like a reference to the NIST standards or some other standard that could evolve over time to ensure that reasonable and strong encryption is used.

Mr. STEARNS. Mr. Burton, do you have a comment on that?

Mr. BURTON. Yes, I think that the encryption standard is very important. I think first, as I mentioned in my testimony, 18 States

have that unencrypted information in the definition of their laws, and I would note that those include Florida, Texas, and Tennessee. And I think that encryption is perceived often as a complex issue. The way these States have mentioned it, it is not a mandate: it is a voluntary action, which provides a safe harbor. And I think this is especially important for mainstream companies who do not understand the world of cybercrime and protecting digital information, and it gives them a straightforward way to go in, protect their data, and know that they have some sort of safe harbor. And if that is associated with NIST standards, then Congress can rest assured that it is good, solid encryption.

Mr. STEARNS. So if you were writing the bill, would you mandate that we use the National Institute of Standards and Technology as a guide?

Mr. BURTON. I would. In my formal testimony to this committee, I included a definition of encryption, which references NIST standards, which has been endorsed, actually, by the Cybersecurity Industry Alliance.

Mr. STEARNS. Okay.

Mr. BURTON. And I think I would include that definition in the legislation, yes.

Mr. STEARNS. Ms. Maier, you suggest changing the definition of security breach, eliminating the need for an FTC rulemaking. But you also state in TRUSTe's guidelines that those guidelines are intended as a first draft and that security policies and procedures need to change and evolve as technologies and businesses do the same. By that logic, wouldn't it make sense to allow the FTC to do this by rule so that the FTC can modify the standard in the future if it is necessary?

Ms. MAIER. Chairman Stearns, yes, I agree that I think the FTC can find positive and good ways to provide the rulemaking that does provide for the flexibility and the evolution of the rules. So I would agree, yes.

Mr. STEARNS. Okay.

Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman.

Let me begin with you, Ms. Maier.

You mentioned in your remarks that TRUSTe works closely with the California Office of Privacy Protection and its ongoing efforts to provide guidance to businesses and consumers on privacy and security issues. First of all, I want you to elaborate a little more on that, but how did these 1,500 companies become affiliated with you?

Ms. MAIER. Thank you for asking that question.

TRUSTe has been around since 1997. Companies who want to show to their consumers as well as to others that they take privacy seriously voluntarily join the TRUSTe program and subject themselves to our standards. And our standards require a very good privacy statement, disclosure about their practices relating to the data that they collect on their website, that they abide by reasonable security standards, and provide provision and choice to consumers regarding the sharing of their information. And so it has been a successful program with 1,500 companies joining in and subjecting themselves to the standards. We developed the security guidelines

to help them define what is reasonable security, and that has also been very successful.

It makes sense for us to work with the California Office of Privacy Protection, because many times, as you well know, a lot of legislation comes out of the State of California and has very broad impact, and we have enjoyed a good relationship with them serving to help develop some guidelines, not rules, per se, but guidelines for businesses in terms of the practical implementation of these rules. And our experience in California in our relationship with the California Office of Privacy Protection suggests that the California law is working, and it is having a positive impact in two ways: one, in providing consumers with notice of breaches and some redrafts and information in terms of what to do under that notice; and two, providing a market incentive for companies to put into place better security.

Mr. TOWNS. Thank you. Thank you very much.

Mr. Hintze, what is your position on broader legislation that it would better inform consumers about who is using their personal information and how?

Mr. HINTZE. We recognize that as a result of the recent security breaches that have been publicized, there is an increasing concern among consumers that they simply don't understand how their data is collected and used and transferred among different entities, and there is a lack of transparency there. We believe there is an appropriate role for legislation to address those broader issues, and we look forward to working with the committee on developing the right rules around that.

Mr. TOWNS. All right. State Attorney Generals have played an important role over the past few years on data security issues. Does Microsoft believe that State Attorney Generals should be able to enforce the Federal legislation?

Mr. HINTZE. Yes, we do. Similar to the approach that was taken in the Can Spam Act, we think that State Attorney Generals have an important enforcement role, and we would support an addition to the discussion draft that would make that clear.

Mr. TOWNS. All right.

Mr. Hoofnagle, regarding your concerns with our draft, what are your thoughts on the feasibility of general privacy restrictions? How can we work to structure the limit of the sale of information, which is a problem, as you indicated?

Mr. HOOFNAGLE. Representative Towns, thanks for asking that question. It is very difficult to describe data protection in 5 minutes, but the common denominator for data protection are fair information practices. These are rights that limit the collection of information to the minimum necessary to engage in a transaction. They are rights to give you access to your data when they are held by companies, a right to correct your data when it is inaccurate, and a right to have your data deleted after a certain amount of time when it is no longer relevant or needed for business purposes. These rights are present in many nations' laws, but to this date, the United States has not adopted these types of restrictions in the private sector. They do apply to the Federal Government, however, and the Privacy Act itself has many of these fair information prac-

tices to stop the government from creating a data center on its citizens.

Mr. TOWNS. All right. Thank you very much.

Let me ask you, Mr. Burton.

In your testimony, you state that you believe that if data is encrypted, companies should be provided a safe harbor and not be required to disclose when there has been a breach of security. Do you believe this should be the case when the compromise of information was due to an insider who has the key to the encryption? Couldn't an insider provide the key to the same people he or she is selling the data to? Or how should encryption protect against insiders who are accessing and perhaps selling personal information that they shouldn't be selling?

Mr. BURTON. That is a very good question, Congressman, and one which was alluded to earlier.

I think the way that I would use the term encryption, and I think the way that all of the States use this term, is if you have a key, the data is not encrypted. Whether I am an insider or an outsider, if I have the encryption keys, I can, therefore, unlock the data, and then it is clear text. So the encryption safe harbor would only apply to data for which one did not have the keys and therefore it was still encrypted. And I will give you an example. Actually, I think it happened in the State of New York. Time Warner had disks. 600,000 of its employees were compromised. Those disks, had they been encrypted, you know, they were lost in transit. And that would not have had to have been reported, because the data would have been scrambled. Similarly, I think there are something like 50,000 laptops which are left in airports around the country today. It is very easy to encrypt the data on those laptops. It is not expensive. It is not complex technology. If those are encrypted and lost, the person who is going to find those will not have the keys, and therefore the data would be safe.

Mr. TOWNS. Thank you very much.

Mr. STEARNS. I thank the gentleman.

Ms. Blackburn.

Ms. BLACKBURN. Thank you, Mr. Chairman, and thank you to the witnesses.

You know, I find it really interesting we are sitting here having this discussion, and a decade ago, there was PGP and the troubles that surrounded that and the designer of that technology and application. And of course, we all know what happened with that. And the government didn't want that application taking place, and now we are sitting here talking about how government wants files encrypted and data protected, and it is for privacy concerns. And so it is an interesting debate and an interesting discussion.

I do have several questions. I know I am not going to get through them, and I will not be here when we do a second round, so I am going to submit some questions to you all.

Mr. Hoofnagle, I think I am going to begin with you.

And let us talk about the misuse to which you spoke, because as we have worked on the identity theft issue and the piracy issue with our constituents, this misuse, as you mentioned, does come up regularly. And have you all noticed any attempts by foreign cor-

porations or businesses or governments to try to buy data on Americans from any data brokers?

Mr. HOOFNAGLE. We at EPIC have extensively used the Freedom of Information Act to determine how companies like ChoicePoint and Axiom and Lexus Nexus, which are where commercial data brokers buy and sell data. We do not have evidence that these entities are selling data to outside the country. I don't think that there would be any law restricting them from doing so, if they chose to. We do know that the companies have data on citizens of other nations, and sometimes the reverse happens. American companies, or American governments, buy data on citizens of other nations.

Ms. BLACKBURN. Okay.

Ms. Maier, do you have a comment on that, please?

Ms. MAIER. We have not been able to identify absolutely that foreign companies have been able to access or sell or misuse American data. That is not to say it hasn't happened.

Ms. BLACKBURN. Okay. Ms. Maier, let me ask you one other thing.

I noticed in the security guidelines paper that you submitted to us, you reference a couple of European countries in your footnoting there. Do you all work with any foreign governments?

Ms. MAIER. No, we do not have direct relationships with any foreign governments. We do sometimes look at some of the data protection trends happening.

Ms. BLACKBURN. Okay. Great. Then let us talk to those trends for a minute.

How are European countries handling their data security problems? Is there anything there that you all have noticed that would be a good lesson learned for us?

Ms. MAIER. My experience with the European data protection standards is that they have a very strict standard in terms of that individuals own their data and have control. And I think to the extent that this proposed legislation and some of the comments that I think EPIC has provided as well as TRUSTe suggest that we continue to provide individuals with access to their information and ability to change, update it, or redact it. That is a really important lesson that I think we can take from the EU experience.

I also would say that the EU experience has demonstrated, to some extent, that a lack of enforcement hinders the implementation and the incentive to do some of the right things. And I think that we can do a better job here in the United States by actively enforcing and providing incentives for companies to really live up to a higher standard.

Ms. BLACKBURN. Okay. Thank you.

Mr. Burton, one quick question for you.

I think it is fair to say that you and some of our witnesses may differ on how this legislation should apply to individuals who may store and use their personal information. And what I would like to ask you is would it or would it not, do you think, be a substantial economic burden to associations and organizations, like churches and private individuals, who have personal information to implement the requirements of the bill?

Mr. BURTON. I think that is a very good question. And I think in my comments I said that the committee was correct in applying

this to all persons who hold sensitive data. Clearly, if you are a small business, if you are a small non-profit, if you do not have, sort of, a lot of administrative ability, then that is something that the committee should take into account. So I think in terms of size of the data set, size of the organization, those may be some limits that you want to consider.

And Congresswoman, if I can beg your deference for one moment, I would like to go back to encryption, which is an issue that I am obviously focused on. And Congressman Towns, there is one important point that I just wanted to make in following up your question about the keys to encrypted data. And I would just like to alert the committee that if you think Social Security numbers are important, encryption keys are an extremely important part of personal data, because as you rightly pointed out, if you get those keys, you not only get Social Security numbers, you get whatever data is encrypted. And that is why when I submitted a definition of encryption, we very specifically took into account the need to protect those keys. There are lots of encryption schemes that leave the keys in the clear, they are easy to get, and easy to hack into. And so as this committee thinks through that issue, you should pay careful attention to making sure that those encryption keys are protected.

Thank you, Congresswoman.

Ms. BLACKBURN. Thank you.

I yield back.

Mr. STEARNS. The gentlelady yields back.

Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much, Mr. Chairman.

And I guess I am going to pose this question to all of the witnesses. You have already touched on it, and I think, Mr. Burton, in response to Congresswoman Blackburn's own question regarding about size and who would it apply to. As currently written, it would apply to each person engaged in interstate commerce that owns or possesses data in electronic form containing personal information. And we do many things here with unintended consequences, but we are going to go ahead and delegate these duties to the FTC and such. And the first question that they are going to have is, you know, who comes under this jurisdiction of this particular law. And while I recognize that there may be problems in its application to everyone and everything, the way I would like this law to end up is something to the effect of, you know, don't collect it if you can't protect it. And that really should be driving this. And still be practical about it. And that is going to be a really hard balance, and I don't know how we are going to pull this thing off.

So that is my question to each and every one of you, and I know that some of you may want to expand on earlier remarks. Do we have a problem in just defining who comes under this particular net or who we capture in this particular regulatory net, if each person engaged in interstate commerce that owns or possesses the data? We have made some distinction with information and data brokers, which we understand, and we can identify those people pretty easily. But there is a whole lot else happening out there, and we will get to this solution again. But let us start off with this

basic concept on jurisdiction and who comes within it. And we will go with the first witness.

Ms. MAIER. Thank you very much.

We do very much care about the definition of who is under the jurisdiction. As I mentioned in my testimony earlier today, consumers don't care. If your information is breached and it is your sensitive information or your Social Security number, your driver's license, your mother's maiden name, your health records, your financial accounts, it does not matter if it comes from your retailer online or off-line nor does it matter if it comes from, perhaps, the California Department of Motor Vehicles or some other State's motor vehicles or my employer records. So I think it is important that we try to keep the jurisdiction, at least for the notice and the implementation of security guidelines with incentives for security to be as broad as possible. And we recognize some other committees might be looking at their own jurisdiction, for example, or a financial institutions. We applaud those efforts. But to the extent that this committee can apply it broadly and extend it even to government, we think that that would be a very good place. And one reason for that is we think, again, consumers are going to feel violated no matter where it happens. They don't draw the lines as fine as we do. And the second thing is that you really want to provide incentives for everybody to put in proper security.

Mr. HINTZE. We agree that we think the legislation should apply to all entities that hold personal information. A couple of things that we would point out, though, in the position that we have taken on this that would alleviate some of the concerns that you have raised, we have advocated a similar approach under this legislation as is taken in Gramm-Leach-Bliley. As Ms. Maier said, consumers don't care about whether or not the data was breached by a bank, a retailer, or a small business. If the data is breached, the threat can potentially be as serious regardless of the source. And so we would urge the committee to look at adopting a consistent standard with what is currently imposed upon banks and financial institutions under the GLB. We have also suggested a flexible standard here. And some of the factors that should be considered in determining what the right kind of information security program that a business should adopt include the size and complexity of the business and the sensitivity of the personal information that they collect. And so that gives a great deal of flexibility to reduce the burden on smaller businesses and businesses that don't collect the most sensitive personal information. And if we still think that there is a concern around the burden on small businesses, we have suggested in our written testimony, I believe, that we could support an exception for businesses that handle small amounts of information rather than based on the size of the business itself. We think that a reasonable approach might be something like if a business handles less than 5,000 records over the course of a year that there could be a reasonable exception there or a reduction of the burdens there rather than just basing it on small businesses, because a very small business could hold enormous amounts of very sensitive personal information, and it just doesn't make sense to exempt them.

Mr. HOOFNAGLE. Representative Gonzalez, we think that there needs to be very broad application of data security standards, because in previous laws where there have been limited jurisdiction or limited applicability of privacy laws, data brokers and other companies that sell data organize in such a fashion so that they do not have to comply with those Federal laws. And the standard example is the way ChoicePoint and other data brokers are organized to escape some provisions of the Fair Credit Reporting Act. And so unless there is broad application, we risk creating a new industry that fits into a loophole.

Mr. BURTON. Yes, Congressman Gonzalez. I think one could successfully run for political office on the slogan, "Don't collect it if you can't protect it." And I think that you are absolutely right, and the Committee is absolutely right, to focus on the data, not who holds it. And what this legislation does, which tries, and I think in large extent, successfully gets at that question, it is not any data. It is sensitive private data commingled with public identifiers. And it is when you put those two data sets together that there is the possibility for harm.

In response to the Congresswoman's question earlier, I would doubt that most churches hold Social Security number, but if my church is holding my Social Security number and they get hacked, I would sort of like to know about it. So I think there do have to be some limits, some size of data sets, but I think the basic principle embodied in this legislation to follow the data is the correct one.

Mr. GONZALEZ. Thank you very much.

Mr. STEARNS. I thank the gentleman.

The gentleman from Nebraska, Mr. Terry.

Mr. TERRY. You would be surprised what churches have. Most churches now have financial records, because they want you to do direct deposits now, electronic transfers so they don't have to worry about whether you show up on Sunday and put your check in the basket, because it was automatically done on Friday. So we have got to worry about the little neighborhood vitamin store that may have personal information, including health information. So I do agree with the phrase you need to protect the data.

So let us talk about that a little bit.

And Mr. Burton, you have come here with the theme of encryption, and I believe that that is kind of the last defense. And I have had people show me how easy it is to unencrypt or decrypt, and in fact, at the University of Nebraska in Omaha, they went online for me and showed me all of the different downloads that you can get just online that will unencrypt the basic information. So to me, that is the last line of defense. At least you make it tougher, and it is only the real data-miners that are out there that are going to know where to get that technology. The casual user that finds a laptop in the airport probably isn't going to know which sites to go to to get their de-encryption software. But as I also understand, that is free on the Internet, too.

So the issue then becomes the vulnerabilities, and this proposed legislation does talk about redacting. In fact, I think the language in is to mitigate and reduce all of the operating software vulnerabilities, which takes me back to part of a presentation I had

by an IT professor to Microsoft that said that there are literally thousands of vulnerabilities in the operating software.

So to Microsoft, let us talk a little bit about the vulnerabilities that are inherent in the operating software, not necessarily yours, but you do kind of dominate the market in operating software. As I understand there are inherent vulnerabilities that are absolutely necessary to the operation, and sometimes there aren't. How do we differentiate? Because I think the first line of attack is reducing the number of vulnerabilities that hackers or data-miners can use to penetrate the system. So what is Microsoft doing? What do you recommend to us by way of the proper language where we can realistically close those vulnerabilities but yet still have the vulnerabilities? And then my last question is who has the responsibility for us in the legislation? Who do we place the responsibility on? The Acme Data Corporation who has the responsibility of protecting the data directly, because they are the ones that own the data? Or is it somewhere that the owner or the makers of the operating software?

So I will start with you, Mr. Hintze, and anyone else who wants to chime in on that issue.

Mr. HINTZE. Thank you, Congressman.

I would first like to point out that Microsoft does take security very, very seriously. It is our No. 1 priority in software development now. We have invested hundreds of millions of dollars over the last couple of years in retraining our developers, fundamentally changing our development and release processes to make security the No. 1 priority, and those effects are paying off in the latest releases and security patches and updates that we make available free to users online.

Having said that, I would also point out that the highly publicized issues of security breaches we have seen recently have not been results of software vulnerabilities. They have been failures of processes, they have been human error and the like. When software is hacked, and it is impossible to make perfect software. It is an enormously complex undertaking.

Mr. TERRY. Are you worried about the language in the bill that says that the operating software has to mitigate all vulnerabilities?

Mr. HINTZE. I am not familiar with that language in there.

Mr. TERRY. Well, I think that is the intention, and I think we need to work through that.

Mr. HINTZE. Yes, we will definitely work with the committee on those issues.

The other point is that when there is a hacker attack, there is an intervening criminal act going on, and I think it is important to keep that in mind. As I said, Microsoft takes this issue very seriously, and we are working very, very hard with our partners, with law enforcement and others and our consumers to help reduce the problem, and we look forward to working with this committee further on that.

Mr. TERRY. And my last question is who has the responsibility to control the vulnerabilities of the software?

Mr. HINTZE. As I said, we will continue to work as hard as we can to reduce those vulnerabilities and make the software as safe as it possibly can be. And we think it is a joint responsibility

among us, consumers, law enforcement, and Congress in helping to make the consumer safe.

Mr. BURTON. Yes, Mr. Congressman, if I could just comment briefly on your opening statement about encryption.

And first of all, thank you for taking the time to have demonstrations and look seriously at it.

If you look at encryption, there are sort of three pieces to it, and this is why we reference NIST. Are you using a strong algorithm? Is it implemented correctly? Are you protecting the keys? If you do those three things, you are left with a brute force attack in trying to decrypt the data, and that takes hundreds of years. You can't download software from the Internet to do that. And I think once you really get strong encryption in place, as you say, it is a second line of defense, and it is very important.

Mr. STEARNS. Maybe just for clarification, I asked counsel just about what the gentleman from Nebraska was talking about, and I think within the bill, I think what we are talking about is requiring the entity that possesses the consumer data, personal data, to take administrative and technological actions to secure the data, but we are not asking you to restructure the software or restructure things like that.

I am going to ask you, and every member is welcome to a second round here. I am going to go to the heart of where we are in this bill and ask—I am sorry, the gentlelady from Wisconsin. Yes. Sorry.

Ms. BALDWIN. Thank you, Mr. Chairman.

Mr. STEARNS. I apologize.

Ms. BALDWIN. I am going to try, if I can, to ask a series of questions and get all of your perspectives, hopefully with very brief answers so that I can get through a couple of questions, some of which you might have already dealt with in your testimony.

I am wondering your opinion first on whether there should be State Attorney General enforcement added to the bill. And why don't we just go from my left to right, if you wouldn't mind, Ms. Maier?

Ms. MAIER. Yes, we would be in support of State Attorney General enforcement.

Ms. BALDWIN. Okay.

Mr. HINTZE. We are as well.

Mr. HOOFNAGLE. Yes, the Federal Trade Commission has too much to do.

Mr. BURTON. Yes, we support that.

Ms. BALDWIN. Okay. Is there anyone in the panel who thinks that this legislation should be expanded to deal not only with electronic personal records but paper personal records?

Ms. MAIER. If I could comment, I think that, first of all, we are very happy to see that was expanded to all electronic data, not just data collected online. That is the most vulnerable, or that is the most useful, to a hacker. But we would be supportive of expanding it to paper-based data as well.

Mr. HINTZE. As we noted in our oral statement, we support that as well. We think whether data was breached in electronic or paper form, the effects can be just as devastating to the affected individual.

Mr. HOOFNAGLE. Yes, we would agree. There are many cases were sensitive personal information has been on paper and then ends up in a dumpster, thus the phrase "dumpster diving". In California, there was an attempt to expand the security of the breach notification bill to cover paper, but that quest failed.

Ms. BALDWIN. Okay. Mr. Burton?

Mr. BURTON. Yes, we would prefer a focus on electronic data. If you look at the breaches which actually sparked this committee's interest in this issue, they were all electronic, and I think that that really gets at the bulk of the issue, and I think that that is the appropriate focus of the bill.

Ms. BALDWIN. Okay. What is each of your opinion on whether we should have a provision dealing with audit trails for the inside jobs?

Ms. MAIER. Our opinion is that as security policies are adopted, audit trails will probably become part of the internal policy. I am not sure if it is required for a broad Federal legislation. With that being said, I think there are some opportunities, through a safe harbor program, to allow for auditing or encourage it.

Mr. HINTZE. We think that that may not be the appropriate level of detail to get into in the bill itself, but certainly that is something that the FTC could look at in the implementing regulations around the development of an information security program.

Mr. HOOFNAGLE. We support audit trails in part because it was clear in the California hearings concerning ChoicePoint that the company didn't know exactly what information was acquired by the criminals and in fact had to rerun the searches one by one to determine what data were actually obtained. An audit trail requirement would substantially reduce that problem.

Mr. BURTON. Yes, I think the audit feature that we would be in favor of is broader than that, and that is there needs to be an audit of an organization's information security programs and that that is really the most important, because that gets at prevention. And not only does there need to be an audit, that audit needs to be communicated to senior management and the board of directors, because ultimately that then changes the culture, which is responsible for better information security.

Ms. BALDWIN. Okay. What is your position on a provision in the bill that would focus on transparency, some sort requiring security breaches to be reported to the FTC and perhaps put on a public website or some additional transparency about these breaches?

Ms. MAIER. Our opinion is that, first of all, the consumers need to know who are affected, and that should be the No. 1 focus. However, I think that to the extent that any sort of notice, be it public-owned websites at the FTC, in sense companies have better security practices, then we are supportive.

Mr. HINTZE. We think that directly notifying consumers is clearly the best way to get the message to the people that need to know it the most. In terms of public posting through a website or through the press, that should be a provision that is in the alternative notice when direct notice is either feasible or impossible. Having said that, we would not oppose any provision that would require cases where notices are required to be reported to the FTC.

Mr. HOOFNAGLE. Especially if companies are given discretion of whether or not to mail the consumers a notice, we think it is very important that the Federal Trade Commission be aware of all of the security breaches. It is a weakness in the California law that only those who are affected get notice, but the corresponding strength of that law is that all breaches have to be disclosed. So especially if there is going to be a discretion standard, and by the way I think there should be some level of discretion. There should be a check on that discretion by public reporting to the Federal Trade Commission.

Mr. BURTON. Consumers should clearly be notified of breaches. Sunshine is the best disinfectant, therefore public notices of breaches are also very important.

Ms. BALDWIN. Thank you.

I see I have run out of time, so I yield back.

Mr. STEARNS. I thank the gentlelady for asking those questions.

I would like to follow up a little bit on what she talked about. This idea of a State Attorney General enforcement of the Federal statute. This is an area that has probably has the most controversial aspect of our bill. Mr. Burton, your testimony states that Entrust agrees with the preemption provisions of the bill, but some have said that a Federal standard should create a statutory floor and not a ceiling, allowing States to go further, if they so desire. I guess please explain why Entrust believes that a more comprehensive preemption is appropriate.

Mr. BURTON. Well, the concern of much of the private sector is that you now have 18 different State breach notification bills that is multiplicity of standards, reporting mechanisms, penalties, and so what industry is looking to this committee for and the Congress for is sort of a baseline, and I think that is the reason that you will get so much support for your legislation and for preemption. I think given the active interest of States in this bill, you have to allow, and you should allow State Attorney Generals to enforce——

Mr. STEARNS. The Federal statutes.

Mr. BURTON. Yes, the Federal statutes.

Mr. STEARNS. And State courts?

Mr. BURTON. Let us see. I am not a lawyer, and so I would have to take that under advisement and get back to you.

Mr. STEARNS. Well, I am going to ask each of you just to make a shot at it, because what the gentlelady from Wisconsin talked about, we had in the spam, but we did not have it in spyware, and we have taken, in this bill, the same language that was adopted in the spyware dealing with the preemption. And, in our opinion, this preemption is important, but we certainly think there are areas that it could be changed. And maybe I will just go to Mr. Hoofnagle. You might comment on this, too, about the preemption provisions in our bill.

Mr. HOOFNAGLE. We think the preemption provisions should be a floor so that States can innovate new solutions, too.

Mr. STEARNS. So, for example, if California has a higher standard, there would be an exemption for California?

Mr. HOOFNAGLE. No, more broadly, we think, that States should be able to pass new laws when new problems arise. We are here today——

Mr. STEARNS. So we establish the floor of the bill, and then above that, the States. But then wouldn't you be back to having 50 States with 50 different——

Mr. HOOFNAGLE. In most privacy legislation, it preempts at the floor level.

Mr. STEARNS. Okay.

Mr. HOOFNAGLE. And it has not created a 50-State set of laws, when Congress does a good job and passes a good law. The States tend not to try to pass conflicting responsibilities.

Mr. STEARNS. Okay. Mr. Hintze?

Mr. HINTZE. Yes.

Mr. STEARNS. Yes, what is your opinion about what the preemption in the bill is and do you support it?

Mr. HINTZE. We do support it. We also would support an addition that would permit State Attorney General enforcement in Federal court, much like is done in the spam——

Mr. STEARNS. Okay. So you support what is in the spam language——

Mr. HINTZE. Yes.

Mr. STEARNS. [continuing] more so than what is in the spyware?

Mr. HINTZE. In this case, we think that State Attorney General enforcement at Federal courts is appropriate.

Mr. STEARNS. Okay. Ms. Maier?

Ms. MAIER. We are in basic agreement with that as well. Coming from California, we certainly would like to see this law at least meet the standard that California has set.

Mr. STEARNS. Okay. Well, let me ask one last question.

The definition of "information broker" that has been touched on a little bit by the gentleman from Nebraska. And Mr. Hoofnagle, is the definition of information broker in the draft legislation appropriate, in your opinion, and does it sweep in entities that are not information brokers, and does it cover all information brokers? That is another area that——

Mr. HOOFNAGLE. Information brokers are very difficult to define. We have worked——

Mr. STEARNS. Yes, but you have all of the affiliates of American Express. I mean, how much should this bill apply to all of those?

Mr. HOOFNAGLE. In some cases, information is traded in such a way that is consistent with the consumer's expectation. So, for instance, a check-cashing clearinghouse you wouldn't want to consider an information broker. They are affecting a transaction that you requested. Generally, information brokers are companies that obtain personal information, often from public records, but also from private sources, and they sell it to third parties, who are not affiliates. And I think if you craft a definition that applies to companies that are generally selling personal information to third parties and that are not initiated by the consumer, for purposes not initiated by the consumer, I think you limit the field substantially. But you are right. It is a very difficult thing to do, because there are many companies out there that are selling sensitive personal information without telling anyone and without the individual's consent.

Mr. STEARNS. I think we are going to complete our hearing today. I want to thank all four witnesses for their time. And I think it

has been very educational and helpful to myself and our staff on both sides.

And with that, the committee is adjourned.

Ms. MAIER. Thank you.

Mr. HOOFNAGLE. Thank you.

[Whereupon, at 11:32 a.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

RETAIL INDUSTRY LEADERS ASSOCIATION
ARLINGTON, VA
July 28, 2005

The Honorable CLIFF STEARNS
Chairman
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
2123 Rayburn House Office Building
U.S. House of Representatives
Washington, D.C. 20515

RE: Statement for the Hearing Record on "Data Security: The Discussion Draft of Data Protection Legislation."

DEAR CHAIRMAN STEARNS: On behalf of the Retail Industry Leaders Association (RILA), I am submitting this letter for the record of the subcommittee's hearing entitled "Data Security: The Discussion Draft of Data Protection Legislation." We appreciate the opportunity to submit these comments.

The Retail Industry Leaders Association (RILA) is an alliance of the world's most successful and innovative retailer and supplier companies—the leaders of the retail industry. RILA members represent almost $1.4 trillion in sales annually and operate more than 100,000 stores, manufacturing facilities and distribution centers nationwide. Its member retailers and suppliers have facilities in all 50 states, as well as internationally, and employ millions of workers domestically and worldwide. Through RILA, leaders in the critical disciplines of the retail industry work together to improve their businesses and the industry as a whole.

Retailers and their product and service suppliers value their relationship with their customers above all else. Consumers vote with their feet every day by purchasing goods and services from retailers and suppliers that they know and trust to provide the quality, prices and services that they expect.

RILA members are committed to maintaining the security and confidentiality of consumer information. RILA supports a uniform federal standard should sensitive customer information be breached and there is a reasonable belief or actual knowledge that harm has been caused by a result of the breach.

As the Judiciary Committee considers data security legislation RILA asks that the committee consider the following core principles:

- **Preemption:** RILA members are committed to policies and practices that safeguard personal data and records and are in full compliance with the current California data breech notification statute. However, other states and jurisdictions have also enacted or are considering similar laws. While these proposals similar, they are rarely consistent, making the potential for a conflicting and confusing regulatory and legal framework all too real. Complying with various and inconsistent state laws could, in fact, slow down the notification process, create unnecessarily complex internal systems, and add cost to the bottom line. Therefore, RILA supports a strong federal preemption that would create a uniform standard "trigger" for notification and for the type of notification that must occur.
- **Trigger:** RILA members believe that notification should only be "triggered" when it is determined that there is, or there is a reasonable belief that there is, a significant risk of harm to consumers. We would note that this is a similar standard supported by the Federal Trade Commission in testimony it has presented before Congress this year. RILA members have legitimate concerns about over notification and believe that clearly defining an appropriate trigger is fundamental to achieving meaningful consumer notice.
- **Covered Data:** Proposals should be limited to unencrypted computerized information.
- **Notification:** RILA members support a uniform notification standard through direct mail or email and are opposed to redundant and costly notification requirements that would do little to increase awareness. RILA also supports a sub-

stitute notification delivery method—email, website, local media, etc.—if notification costs would exceed $250,000 or the breach affects more than 500,000 consumers.
- **Private Right of Action:** RILA supports data security legislation that would prohibit individual private rights of action.
- **Credit Freeze:** RILA has concerns regarding the impact of so-called credit freeze proposals that would allow consumers to place a freeze on their credit report. While proposals of this nature have the biggest impact on the credit agencies, retailers, particularly those who provide instant credit, are concerned about the spill over effects of credit freeze requirements. When a customer freezes their credit file they are likely to forget to "unfreeze" their file before they apply for instant credit creating consumer frustration and confusion when instant credit cannot be issued. In addition, retailers are concerned that additional credit agency requirements could drive up the cost of credit reports. While the industry has concerns with credit freeze requirements, if provisions are adopted, there should be a uniform national standard.

With regard to the draft document that the committee is considering at today's hearing, we have prepared the attached comments, which we have previously provided to the subcommittee staff.

If you have any questions about this matter, please don't hesitate to contact me or my colleague Lori Denham, Senior Vice President, Policy and Planning.

Sincerely,

PAUL T. KELLY
Senior Vice President, Federal and State Government Affairs

Attachment

RETAIL INDUSTRY LEADERS ASSOCIATION GENERAL COMMENTS ON BARTON/STEARNS DISCUSSION DRAFT "DATA SECURITY & SECURITY BREACH NOTIFICATION"

JULY 28, 2005

Security Requirements for Data

Section 2

- Rules promulgated by the FTC may require specific policies and procedures that may or may not be appropriate for the protection of the personal information maintained by companies. While we support the idea that companies should have policies and procedures in place to protect personal information, we believe individual companies are in the best position to determine what form those policies and procedures should take.
- RILA supports an exemption for data that is encrypted.

Nationwide Notification for Material Security Breaches

Section 3

- Breach of Security. We agree with the concept of risk assessment in determining whether a notice of breach to consumers is necessary. Inundating consumers with notices regarding a breach of information when there is no evidence that the breach has, or will, result in identity theft is counter-productive. There is a real danger that over notification will result in consumers becoming numb to the notices and they will, therefore, fail to take necessary steps to protect their information.
- Timeliness of Notification. Many of the state laws regarding security breach notification have included a provision that would allow for the delay of notification to consumers in cases where law enforcement requests a delay so they can complete an investigation.
- Method of Notification. Notification by mail and email and web site could prove burdensome. We would support a notification scheme whereby individuals could be notified by mail or email and by the posting of a notice on the company's web site. It is not necessary to notify consumers by both mail and email. Companies should be able to choose the method that is most practical and efficient depending on the circumstances. Providing notice on the company's web site would then be an appropriate and practical addition to the mail or email notification. If a company chose to send notice by email, it should be allowed to do so without having prior "consent" from the consumer to receive such messages. This would be an operational (not a commercial) email message and one that consumers would want and need to receive regardless of whether they had previously provided consent.

Definitions

Section 5

- "Personal Information". The definition of personal information is consistent with the definitions established in California's (and other state's) security breach notification laws. If this definition is acceptable, why would the Commission be allowed to modify it in the rulemaking?

Effect on Other Laws

Section 6

- The preemption language is limited to "...breaches of security of data in electronic form." State laws have contemplated breaches in forms other than electronic. The preemption should be complete so that companies can implement one security breach notification process. Companies should not be put in a position whereby they have to follow specific state laws for information that is maintained in forms other than electronic.
- Banks, credit unions, thrifts and common carriers are exempt from coverage because they do not fall under the jurisdiction of the FTC. However, these entities would need/want to take advantage of the preemption provision. If these entities are not included in the preemption provision they will be subject to federal regulatory guidance and the myriad state laws that address security of information and notification in the event a security breach occurs.

Effective Date and Sunset

Section 7

- What is the reason for attaching a sunset provision to this legislation?

For more information, contact Lori Denham, Senior Vice President, Policy and Planning (703) 600-2012 or lori.denham@retail-leaers.org or Paul T. Kelly, Senior Vice President, Federal and State Government Affairs (703) 600-2014 or paul.kelly@retail-leaders.org.